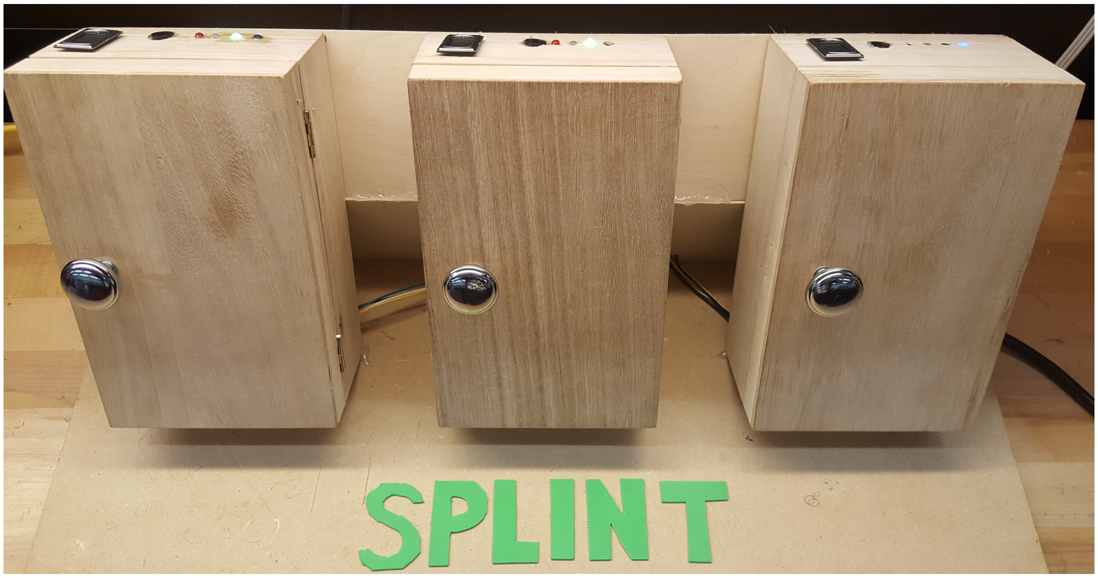


Senior Design – Group D
Secure Phone Locker with Integrated Notification Tracking

Department of Electrical Engineering and Computer Science
University of Central Florida
Dr. Lei Wei

Project Design Team:

Alexander Masterson	**CpE & EE**
Ian Flemings	**EE**
Nick Lucas	**EE**
Evelin Santana	**EE**

Possible Customers:
Academic Centers, Businesses, really any facility with a public outdoors area.

Sponsors:
None at this time.

Significant Contributors:
None at this time.

Table of Contents

Table of Figures

Table of Tables

1.0 Project Executive Summary

Our goal is to create a charging remote alert notification station. The idea of the project is to create a device that allows for people to go to work, place their phone into a chamber, and leave it there until the end of the day. The chamber will have devices in it that make sure it is secured and can't be stolen, charge the phone, monitor whether or not the phone is receiving texts and calls, and then alert the people at a designated work computer that they have been contacted. The owner of the phone will be able to see alerts on a designated work computer and make a judgment call on whether or not they need to take the time to check their phone or wait until a break or the end of their work day. This project is really useful for companies that have restricted zones where workers are not allowed to bring a personal phone into the area, but have a dedicated computer in the area, or a person who monitors the areas and has the ability to communicate with them. It alleviates some of the inefficient walking out of the restricted zone to check a phone periodically if an employee has to be watching for a call, such as a parent waiting for a call from their child, or a person who is waiting on an important business call such as a lab head. The product will also be good for those cases where people who have to put their phones in a designated location sometimes leave their workplace forgetting their phone due to the stresses of a long day. The system will keep their phone secure until the owner can come back and retrieve it.

This system can ideally be used in two different ways. Either employees will walk into their work space, place their phones into the device, or then there is a communal computer/monitor where the employees will be able to see notifications show up. Employees will be able to match a box number shown on screen to the number of the box where they placed their phone. That is one way, the other ideal way is that employees will walk through the lobby of their workplace, and the receptionist will have a terminal and device assembly next to them, The receptionist will request all employees to drop their phones off at a designated box number and the receptionist will keep a list of employees and what box their phone is currently being stored. As the terminal receives notifications, the receptionist will be able to forward those notices to the employees via an intercom or email.

In essence, the device itself will work by allowing a user to place their phone into an observed box, and then scanning their fingerprint. That fingerprint will be stored and then the box will be mechanically locked from the inside. The box will not open again until the same user who originally scanned their fingerprint goes to the device and scans their print once again, essentially preventing outside and unauthorized users (anyone who isn't the owner of the phone) from getting access to that device. The observed box the device sits in has various sensors to monitor when the phone vibrates or lets off a sound, which are common indicators of a mobile phone recent a notification of some type. The observed box will then listen in on these stimuli and send alerts to the designated terminal telling the terminal that a phone has emitted a type of signal and in what box that phone is currently placed.

It is our hope that this device will be able to help improve overall productivity in the workplace, as well as ease the minds of people who are required by certain workplace procedures to separate from their phones who worry about the safety and security of their devices. In today’s digital world, a person’s phone has become an integral part of their everyday life. People rely on their phones as a way of accessing a massive pool of information, staying in contact with important work contacts and loved, occupying their time with leisure activities during their down time, and several other things. Having that phone on their person can easily be a distraction in professional settings though, but people may not feel comfortable separating from their devices for various reasons. We believe that if we can improve a person’s faith that their devices will be safe, and that there will still be a way for them to address emergencies, then we will see an improvement in overall workplace efficiency as we have removed a large demand on the employee's attention, and that is the end goal.

2.0 Project Introduction

In this chapter, we will cover the contributing factors that lead us to choose our charging remote alert notification station project. We will discuss our motivation and the problem that currently exists. Next layout our objective solution and goals we hope to achieve with this project.

2.1 Motivation

The idea of the project is to create a device that allows for people to go to work, place their phone into a chamber, and leave it there until the end of the day. The chamber will have devices in it that make sure it is secured and can't be stolen, charge the phone, monitor whether or not the phone is receiving texts and calls, and then alert the people at a designated work computer that they have been contacted. The owner of the phone will be able to see alerts on a designated work computer and make a judgment call on whether or not they need to take the time to check their phone or wait until a break or the end of their work day. This project is really useful for companies that have restricted zones where workers are not allowed to bring a personal phone into the area, but have a dedicated computer in the area, or a person who monitors the areas and has the ability to communicate with them. It alleviates some of the inefficient walking out of the restricted zone to check a phone periodically if an employee has to be watching for a call, such as a parent waiting for a call from their child, or a person who is waiting on an important business call such as a lab head. The product will also be good for those cases where people who have to put their phones in a designated location sometimes leave their workplace forgetting their phone due to the stresses of a long day. The system will keep their phone secure until the owner can come back and retrieve it.

We came up with the idea after observing the inefficient phone handling system that a D.O.D. manufacturing facility had for their restricted labs. They had open shelves outside of the door where people just haphazardly placed their phones. Sometimes phones fell off the shelf as the door was opened and closed and got damaged, lab technicians wasted time having to go through the lab exit process simply to check their phones and see that they have not received any notifications or they are checking on their phone to make sure that their phone hasn't suffered an accident due to another person. We have also heard the story of people walking out of the lab, forgetting their phone on the shelf, and then the phone goes completely missing because some other person moved it before the owner could get back to it.

2.2 Objectives

Our objective for this project is to create a modular system that can safely keep a phone charged for the duration it is in the chamber. The system should be able to securely lock in the phone until an owner can provide an authentication. It should be able to maintain a charged phone, and not block the phone from receiving phone calls or messages. We want the system to be able to accurately measure disturbances such as sound and vibrations in order to determine alerts. We also want the system to be able to communicate a secure terminal inside the facility to relay alerts that have been detected. We want the system to function without the use of radio frequencies to accommodate facilities where radio frequencies create bothersome interference.

2.3 Goals

Our goal is that we want to see this product being used in businesses to improve overall worker productivity. We hope to see this product remove some of the distractions associated to people checking their phones all the time, but at the same time, maintain the important function of being able to be notified if emergencies. We mainly hope to see this device used in fields where users have to sacrifice access to their mobile devices, their primary source of long distance communication with others, in favor of environment safety. Eventually we would like to expand this device to be large enough to accommodate for entire facilities of people, rather than just small groups.

2.4 Existing Technology

There are wireless charging stations currently in the market who use inductive charging technology. These stations also have added features such as temperature control to keep the device safe and power-efficient idle mode so that your device doesn't over charge while docked. There are also some with docking stands and smart LED indicators for ease of use. There are also universal wireless charging receivers which will connect to any android phone via your micro-usb port on the phone and then connect with any charging station, this is useful in case you don't have a phone that automatically is made to connect to the specific charging station. While there are many charging stations that offer secured locking and efficient charging, none that we came across offered an emergency notification system. This is where our product fits in, we intend to add degree of functionality that is not currently available on the market which should carve out a market within secured facilities that wish to do more than just charge. This device will subvert problems that RF in phones can cause in certain situations by removing the phones from the situation, but allowing users to still be aware of their cellular devices.

2.5 **Block Diagram**

The diagram below shows an overall overview of the different functional blocks that the system we are proposing will need and use. The diagram also shows a general summary of which functional blocks the members of our group will be chiefly responsible for.

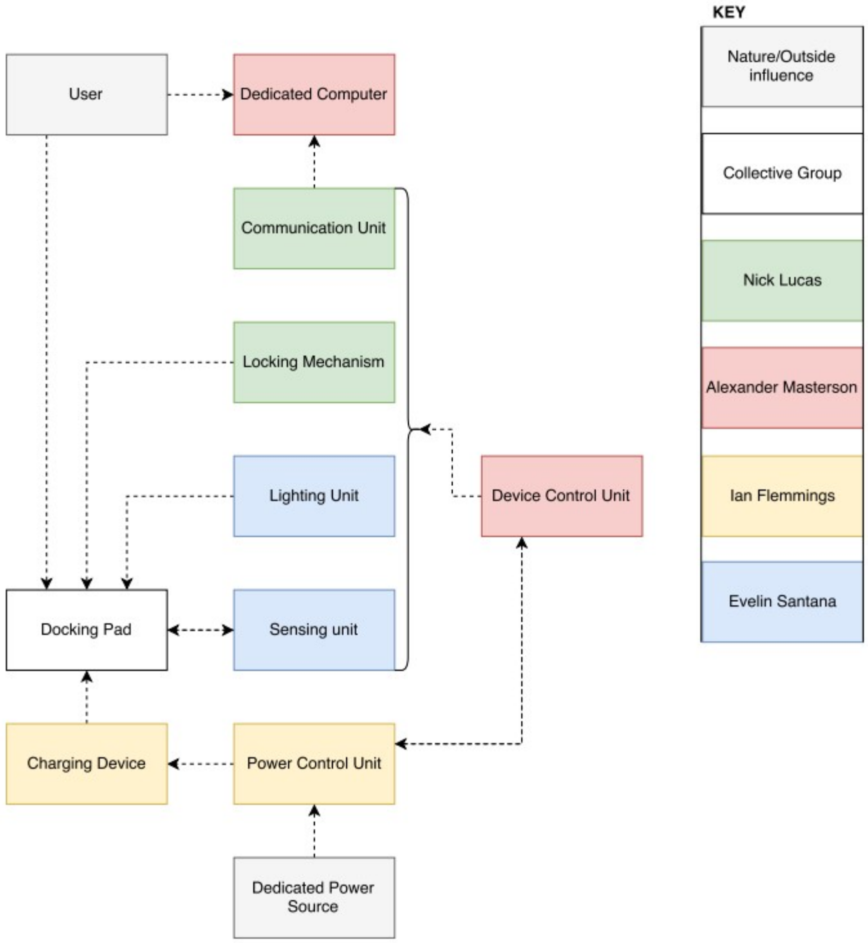


Figure 1 - Low Level Block Diagram

Items in gray are what we are considering forces and important functional blocks that are beyond the control of our group in the development process. We as product developers cannot control whether or not a user or a monitor actually uses the devices. We also cannot control what devices are also implemented into the power source. These are simply things we are making assumptions about during the development process.

Items in white are what we are considering the collective effort blocks of the group. These are the blocks that are brought together by the different parts managed by all members of the group. In essence, these blocks are complete assemblies of multiple parts. The only white block is the block for the docking station.

Table 1 - Block Diagram Overview

Function Block	**Function Block Description**
Charging Device	This is one the main devices of this assembly. This device is in charge of facilitating the charging of phones inside of the unit. This will allow the phone to be active for the entire time it is in the enclosure so that the other devices in the assembly can make sure that the user doesn't miss a single alert.
Communication Device	The idea is to have a dedicated computer with an application on it that this device communicates with. We are proposing that this device sends alerts to the dedicated computer. This block is in charge of facilitating the successful formatting and transfer of data from the device to the dedicated computer.
Dedicated Computer	This is the device that receives messages from the communication device. The idea is for this dedicated computer to receive messages from the communication device and an alert will show up on screen. Then a person in a restricted area can look at the computer and see the alert, or a person monitoring the phones can look at the alerts and forward it via a speaker system or some other method.
Device Control Unit	This is the center of operation for the entire product. This unit will be the thing that monitors any inputs from the sensing unit, controls the lighting unit, verifies the authentication for the locking mechanism, actuates the locking mechanism, processes data from the sensors and then sends data to the communication device for transmission.
Lighting Unit	This is the station responsible for the lighting system. There will be LED's along the docking pad to indicate that the phone is active in the docking station and it will also serve as decoration to make the device look more appealing.
Locking Mechanism	When a person puts their phone into a docking pad, they are going to want the phone to be secure. This block handles the physical device that secures the phone. This block also handles the input for the authentication method the device employs.
Power Control Unit	This block is the heart of the product. This is the block that handles how the entire product is powered. The main purpose of this block is to take in power from a dedicated power source, regulate it, and distribute the proper amounts of power to the different loads in the overall system. This block also handles any necessary input power protections.
Sensor Unit	The main draw of this product is that it monitors your phone and keeps your updated about alerts while you are in areas where you are not allowed to have your phone. This block handles all of the sensors that do just that. This block handles the sensor inputs and the transmission to the device control unit.

3.0 Research

In this section we will cover all of our research for the project. We will detail the power requirements and considerations that will be need to be accounted as well as the design methodology that we used to design the power distribution throughout our project as well as determine which power supply we will be using for our design. We will also cover our communication and transmission network topology design considerations and the information that will lead us to the specific topology that we consider to be the best option for implementing our project.

We will go into detail that different analog and digital sensors that can be used for sensing vibration, sound, and door position, and make comparisons between the different types of sensors. We will then decide which sensors will be used in the various portions of our project, and select which sensors we will ultimately use for our design based on our needs and the specifications of the sensors. Once we have the sensors picked out we will compare some microcontrollers and determine which would be best for processing and controlling the inputs and outputs of the sensors.

We will have a section that covers our physical security needs when it comes to our locking mechanism and authentication. We will compare and contrast the different types of locking mechanisms that are available for our design, and after selecting the type of mechanism we will be using, we will again compare specific products of that type to make a decision on the best mechanism to use in our design. We will also investigate the various forms of authentication that are available, detail how they are used and how they might be implemented in our design. Once we have compared and contrasted the various forms of authentication methods we will narrow down which implementation would be best for our needs and requirements, and we will compare available products and decide which we will move forward for our prototyping. Finally we will compare and contrast some microcontrollers that might be used for the security and authentication and make a selection on which will be used.

Lastly we will also delve into materials and methods that can be used for isolation and damping purposes between the chambers of our systems. This is one of our unforeseen challenges to meeting our engineering requirements and design specification. We will explain some different damping and isolation methods and follow up by determining which method or materials would be best to use for vibration and sound damping between chambers.

3.1 Power

This is the section where we will discuss the power requirements that our design will have and the considerations we must make as we design how the power will be distributed. We will also go into detail how the voltages will be transformed and rectified, as well as how the switching will occur and the design structure we will use for this implementation.

3.1.1 Power Requirements

In this section we will detail the power requirements and how each will effect our overall design.. Since the majority of our parts are going to require a fair bit of precision, and we have varying parts, it will be necessary to have our power circuits be very well regulated. Looking at a general overview of the circuit, there will be certain things that require a bit more precision than others. In Descending order: The USB interfaces (by NIST standards),The active sensors, the MCUs, and lastly the latched locks.

3.1.1.1 The USB interface

In addition to our other circuits, standardization limits more than just voltage for the USB chargers, it also puts a restriction on the current. It is important that we add a current limiter before the output for both NIST standards, and as a backup plan to prevent phones from drawing too much current and heating up the LIPO battery beyond its threshold point. USB uses a 5V, 2.5A standard, and for our purposes we are likely going to be limiting the current to about 2.1A for good measure, and regulate power rail voltage to 5V as best we can.

3.1.1.2 Active Sensors

The active sensors require a more precise voltage due to repeatability. Even if the sensors have a high tolerance range, the given output will change dependent on a given input, and if our sensors have a high variance in supply voltage, then we will have variance in the output. [experience] Given the task we have set out for ourselves, it is important for our thresholds to be as repeatable as possible. [foresight] Currently, we're regarding the fingerprint scanner within the active sensors category. [laziness]

3.1.1.3 MCUs

It is not uncommon for certain MCU's to have onboard regulators, but even in those MCUs having a voltage offset from the nominal voltage causes excessive heating and power loss. If we can be efficient in regulating the voltage of the MCU then we can minimize the heat generation and power loss. Since our only consideration is being within operating range, and ensuring consistency, this is not nearly as important as the Sensors or the USB power supply.

3.1.1.4 Latched Locks

The least important item on the list will likely be the latches. If we use latched maglocks, we will only need to supply a voltage of at least 12V, and an amperage to activate the electromagnet for a temporary period to change states. Since these are two very discrete states, there isn't much precision necessary. Because of this, the least regulated device in the circuit will be the latches.

3.1.2 Design methodology

In this section we will discuss the main design needs and how each one will be addressed. We will detail how we will address each need and explain how each subsystem design functions.

3.1.2.1 Mutual Inductance Transformer

The first requirement in using standard 110/220AC in a low power, DC circuit is to step the voltage down. What we will first want to do is step the current down from standard 110VAC to about 12VAC. One of the most common implementations of this is mutual inductance, which uses coils that are magnetically coupled (usually through some medium) and then uses the a time varying voltage to induce a magnetic field and generate a voltage on the other coil. [3] Figure 2 acts as a visual aid to show a simple mutual inductance example. Note how the two circuits are not actually in any direct contact.

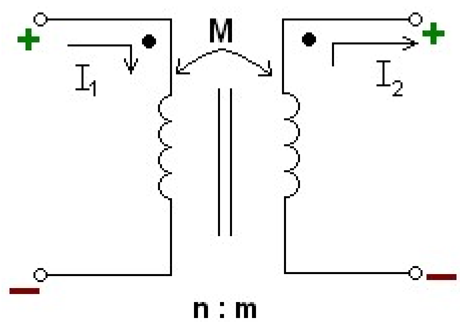


Figure 2 - Simple Mutual Inductance

Mutual inductance transformers are a very nice way to drop the voltage in an AC circuit down, while minimizing the power loss. For simplicity, the equation for the output voltage of an ideal transformer is Vout = (N2/N1)*Vin, where N1 and N2 are the number of turns on the input and output coils respectively. [3] If we decide to create our own transformer Rectifier power circuit, we will have to consider the many non-ideal considerations of a mutual inductance transformer, such as copper loss and eddies.

3.1.2.2 Rectifier/Bridge

The next step will be rectification of the signal. The simplest rectifier is a half-wave rectifier, essentially cuts out half of the circuit by placing a diode on the positive end, and allowing the cutoff region to prevent any voltage of opposite polarity from passing. Figure 3 acts as a visual aid showing the input, output, and circuit design of an ideal half wave rectifier.

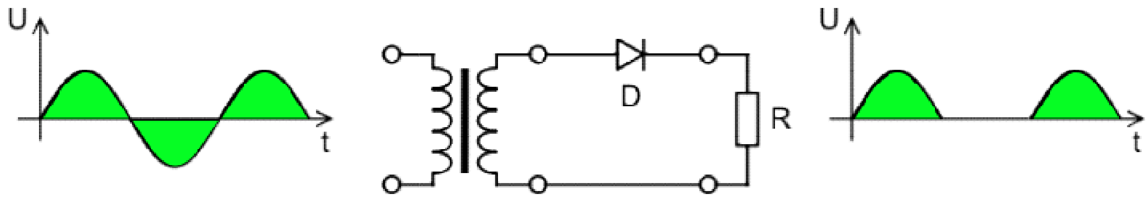


Figure 3 - Input, Circuit Design and Output of a half wave rectifier.

Even under ideal circumstances, it only allows the signal to pass half of the time, and reduces the power passed through it. An alternative, and the next logical step for a full-wave rectifier, is a Graetz bridge rectifier, which uses the same idea in a half-wave rectifier, but also adds a diode to the negative end of the load in the opposing direction, and duplicates a similar circuit in the opposite direction for the opposite path. Figure 4 acts as a visual aid showing Graetz bridge full wave rectifier inserted after a transformer.

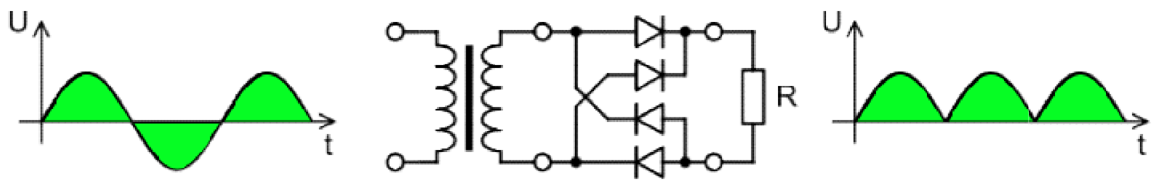


Figure 4 - Graetz bridge full wave rectifier

The last classic design option involves a modification to the transformer. If a center tapped transformer is used the center tap would then be the ground and there would be no necessity of the extra return loop diodes. This would require a different type of transformer, but would allow for a slightly simpler design, with fewer power dissipating elements, at little to no cost to the power transfer of the transformer [4]. Figure 5 shows a Full wave rectifier using a center tap transformer and 2 diodes

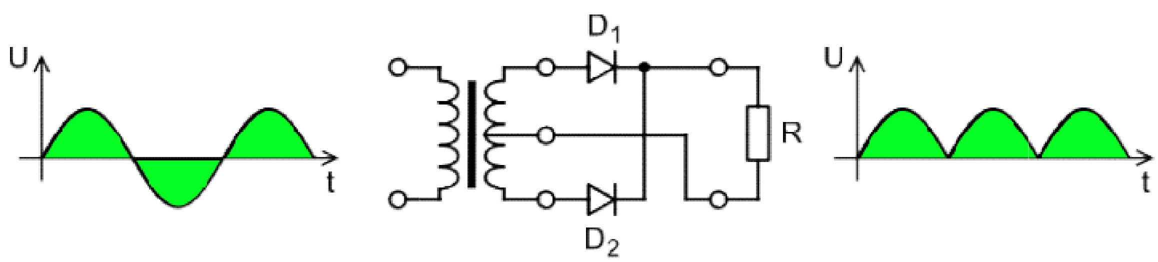


Figure 5 - Full wave rectifier using a center tap transformer and 2 diodes

3.1.2.3 Smoothing Capacitor

A smoothing capacitor, in one interpretation, operates under the condition that a capacitor cannot have any instantaneous changes in voltage. [4 years of college] With appropriately chosen capacitors, you can smooth out the voltage by ensuring that the capacitor cannot discharge a certain amount in the time it takes to get from one peak to another peak. Capacitors will also inherently create a low pass filter, and filter out any high frequency noise, which is what most electrical noise is. Figure 6 shows an example of using a smoothing capacitor on a half-wave rectified signal. The signal without the smoothing capacitor is shown in black, and the signal with the capacitor added is shown in red

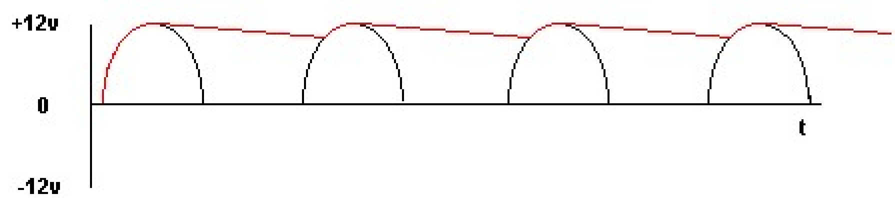


Figure 6 - Using a smooth capacitor on a half-wave rectified signal

3.1.2.4 Voltage Regulators

Voltage regulators are electronics used to maintain a certain voltage. There are many different implementations of voltage regulators, but its most common to use solid state voltage regulators in low-power circuits, as they are compact and efficient.

There are generally two different types of regulators, Linear and Switching. [5] [6] They both have their pros and cons*, generally switching regulators are considered to be more efficient, however, these chips tend to be more bulky, noisy, and expensive if they tend to be low powered circuits.

3.1.2.5 Switched Mode Power Supply

Modern Transformer designs use a switching mode power supply (SMPS), which is significantly more efficient than a regular linear power supply. Switched mode power supplies are devices that are continuously switching “on” and “off” with high frequency in order to provide the transfer of electric energy through inductors and capacitors.[1] switching mode power supplies are very complicated circuits and require a great deal of design considerations by themselves. if we were to implement this, it would likely require a great deal of foresight and take up a lot of time of one of us! Ideally, it would be much better to implement an SMPS as a mains converted over a linear power supply due to its efficiency alone.

3.1.2.6 The basic design:

Our current design is a module one that allows for extra boxes to be added at ease, and to allow each box to be repaired or replaced with minimal interruptions. Currently the design idea is to keep the differential on both sides of a voltage regulator (VR) as minimal as possible, while minimizing the total amount of power being transferred across any single VR. While the Power supply circuit from the last smoothing capacitor on can easily be replaced with a simple 12V power supply, it’s worth mentioning that given the time and ability a switched mode power supply may be a better design. The compartments will each have rails the slide into the base, with an *n* (at least 4) contact bus. One directly from the power supply, and one after a series of voltage regulations. Each compartment will provide power for the MCU, the USB charging, and any active sensors we may have.

3.1.2.7 Approximated voltage of possible devices

Since most of the devices involved in this system are precise, typically low voltage devices, it is important for us to keep track of the voltage requirements:

Table 2 - Voltage Requirements

Thing	Min	Max	Unit
USB Standard	4.75	5.5	V
USB Standard	1.0	2.5	A
atmega328	1.8	5.5	V
msp430F1xx	1.8	3.6	V

3.2 Communication and transmission

This section will cover the communication topology and communication microcontroller considerations, as well as the cable considerations that come into play when designing out system.

3.2.1 Communication Topology

Since our communications have varying degrees of distance, and varying amounts of information, we must consider distance, and topology. One consideration would be a pure MCU topology shown in Figure 7. A second consideration would be an Ethernet network topology as shown in Figure 8. Our most likely consideration would be the formatted network interface shown in Figure 9.

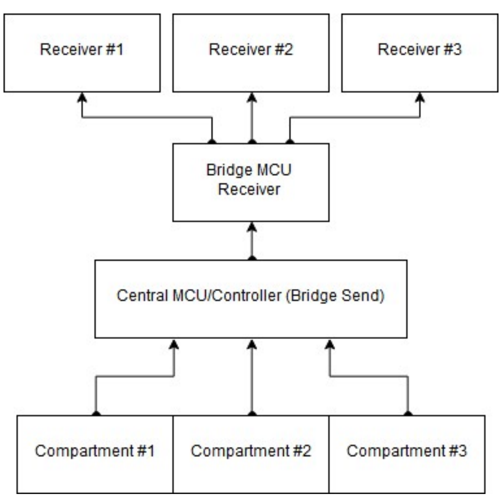


Figure 7 - Pure MCU Topology

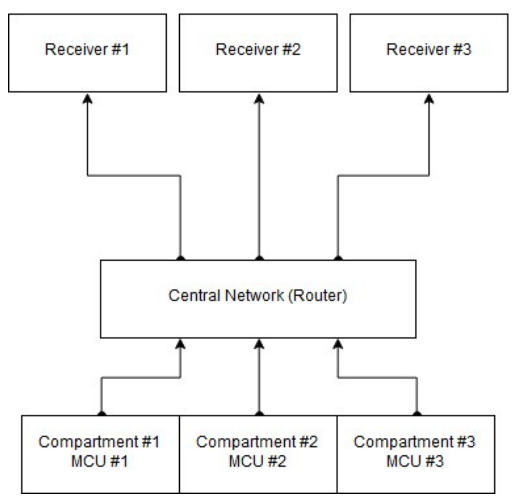


Figure 8 - Ethernet/Network Topology

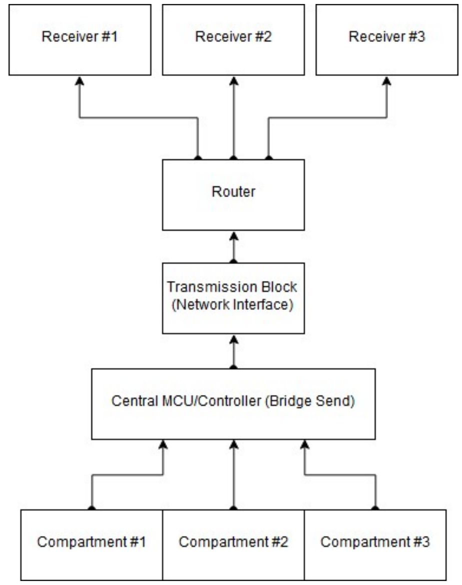


Figure 9 - Formatted Network Interface

At least one of these involves long distance communication over a non-standard methodology. Note (Any one of these communication lines can be bussed)

3.2.1.1 Type of Cable considerations

Long distance and short distance communications have different accommodations for noise [1] and different means of long distance communication. If we were to use the latest standard transmission mediums, this leaves us with Coax, Fiber, Twisted Pair (Ethernet), which have 550ft, 600ft and 300ft max lengths respectively. [2]

While coax cable is designed to shield from interference and allow for many frequencies [4] they can still undergo signal leakage [5] and will require further research for us to calculate the desired power consumption [6] to accommodate for the required attenuation. [9]

Fiber Optics would be perfect for ensuring no RF leakage, as the channel/medium is one that does not produce electrical interference, as it does not use electricity as the communication mechanism. On the other hand, there are power and cost considerations. [7] [8] [10]

Ethernet (shielded, twisted pair) has standards to reduce the electrical noise it receives, but was not designed to prevent electrical noise. It would be reasonable to assume, however, if the building that would require this device uses Ethernet for networking their computers, that Ethernet would be a viable solution, as it is currently used a long distance networking solution for a number of different MCU's SOCs CPUs and IoT devices as a whole. It would allow for a very quick and easy setup/connection to an already existing network.

3.2.2 Networking Topology

When designing a communication network, it is usually a good idea to start from the top level of the network, and then work down from, consider any nodal constraints, and then work your way down from there. If one doesn't, they're most likely to end up with a partial mesh, which is more commonly something to compensate for not to assist in design.

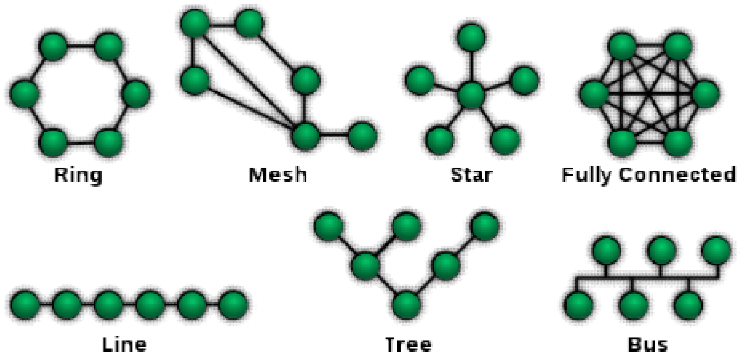


Figure 10 - Generic Network Topologies

To assist in explanation, I've included a diagram that lists some of the most fundamental topologies.

Bus topologies are most commonly used for low level, very-low traffic networks, or networks where every node which has only one tx/rx port. This is typically used in master/slave configurations as collisions are almost guaranteed if there is more than packet being sent at a time. *Low cost of implementation.*

Partial Mesh Topologies are typically used in networks where there is very little control over the context of the network. The internet is a common example of a partial mesh. Cost can vary based on implementation.

Fully Connected Mesh Topologies are just like the partial mesh topologies, except every node is connected to every other node. These are commonly used in very high traffic environments, have a huge cost for implementation, and have the largest complexity per add-on. Full Mesh topologies are not typically used for large networks or networks which have a large number of future additions or changes. This implementation has a high cost.

Star Topologies Are very similar to partial meshes, except all connections are connected to a central node. Because of this, the central node needs to be very robust, and this can also impose many limitations on the network as well. Star topologies have similar cost of implementation as partial mesh networks.

Ring and Line Topologies: Ring and line topologies are very similar in nature. Before we start getting into directional graphs, the only difference between the two is that the two end nodes are also connected in a ring topology. Line topologies are riddled with single-points-of-failure, and bidirectional ring topologies solve that problem by allowing for one connection to fail and still maintain full connectivity. Ring and Line topologies need to be very robust at at least one node, and can become overloaded very easily.

Tree Topology: Tree Topologies have hierarchy, and allow for a many nodes to be organized into smaller groups up until the head node. This allows for less robustness in each individual node, and gives a great deal of modularity to the system. Tree topologies have a higher cost of expense than Line, Bus, or star topologies, but it distributes a network load evenly, and allows for a great deal of management. Tree topologies are most commonly used in modular networks, and most commonly used in high performance, fast growth networks. Tree topology requires a large amount of control over a network at the top level.
Notable points: No network is restricted to having only one topology. There is very little separates certain topology configurations, and very little that prevents one topology to be used in smaller sections of another network with a different topology. These are also very basic topologies.

We're most likely going with a tree topology or tree+bus topology to allow for organized growth.

3.2.3 General Assembly Overview

Below in Figure 11, we are showing the current proposed system assembly using one microcontroller to monitor all of the sensors of an individual observation chamber. The individual microcontrollers used to monitor the sensors will be linked to a microcontroller intended for the purpose of sending messages to an outside terminal. The senor controller will monitor the sensors and when one (or more) sensors detect acceptable input, the sensor controller will send a flag signal to the messaging controller. The messaging controller will then handle those flags, do any processing it needs to do and send appropriate messages to the terminal.

With this layout, the sensor controllers will also have the duty of storing and processing images from the fingerprint scanner. This will make the sensor controllers a little more complex and expensive, but we believe that the improved ease of use to come from this parallelism of tasks will improve user satisfaction when using this product. This will also add programming complexity to the sensor controllers, but adding code to handle a single fingerprint at a time in the sensor controller and then outputting a flag is less computationally complex than having one controller handle fingerprints for all chambers in the device. On top of that, we can essentially duplicate the simpler code for all of the sensor controllers and give the message controller less computationally complex code. This will overall improve development time and cost less memory overall, meaning we can cut costs on getting a controller with a lot of memory.

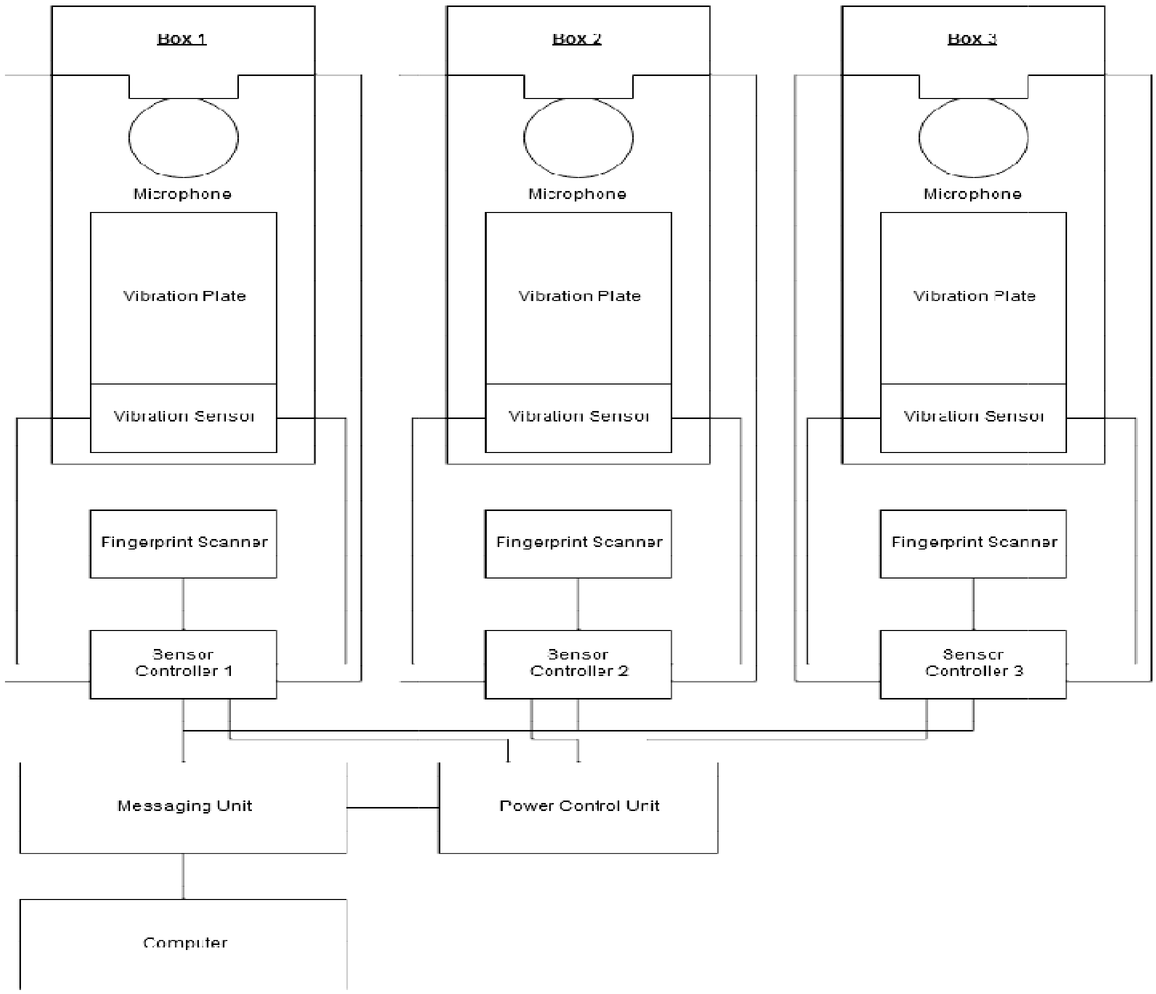


Figure 11 - Proposed General Layout

3.2.3.1 MCU Considerations and Selection

There are several different things that come into play when deciding what we will be using to handle our main communications with a terminal inside. Based on our communication needs we would like to be able to transmit packets of data which would most easily be accomplished with if we use a simple operating system. We would like to be able to take in all of the necessary inputs from the multiple chambers and assign them an address or "name." From there
Ardunio
BeagleBone Black
Rhaspberry Pi
MSP430 (and associated Ti MCU's) Each one has their pros and cons

Table 3 - MCU Comparisons

Board	Pros	Cons
Arduino(ATMega)	Low Cost (~$25)	Strictly low-level
	Open Source	Slow
	Plenty of components designed just for it	Low memory
	Easy to use	
	Low Level	
	Power Efficient	
	multiple Digital and Analog GPIO Pins	
BeagleBone	Open Source	High cost (~$50)
	Low and High level interfaces	Not the most documentation
	Reasonably Fast Processor	
	Many Analog and Digital GPIO pins	
	Ethernet	
	Linux and Android Compatible	
	Video and Audio Capable	
Rhasberry Pi	Fast Processor multicore processor	No analog GPIO pins
	Plenty of RAM	
	USB ports	
MSP430	VERY power efficient	Strictly Low Level
	Plenty of Documentation	Slow
	Small	Low memory
	Many GPIO pins	
	Very Scalable	

[12][13][14][15][16]

We have made the decision to use a BeagleBone as the platform for our communication. It would be our best choice as it has the optimal Ports to CPU power ratio as well as the ability to run an operating system which will be used for interfacing with terminal.

3.3 Sensors

In this project cell phones will be placed inside an enclosure for safe keeping during business hours and sensors will monitor the status of the phone. If it detects that the phone is either vibrating or ringing then it will send an electrical signal to a microcontroller so that the unit can inform the user that they have received a message notification.

A sensor is an electrical device that can pick up changes in the environment from the result of an excitation and can convey that information externally. There are several types of sensors, ones that can detect movement, magnetic energy, temperature, among others but we will be using sound and vibration sensors for this project. There are many choices for sensors, they can be either active or passive, have an analog or digital output. The sensitivity level and whether it affects the information that it picks up are also factors.

3.3.1 Analog vs Digital

When it comes to analog vs digital we need to look at how different they are. An Analog sensor produces a continuous analog output. The output voltage/current is proportional to the change in the environment. Analog sensors usually have 2 or 3 wires: 2 wires for power and a third for output for sensor reading. Analog systems can handle data much faster than digital systems but are limited in their accuracy due to noise problems that affect all electronic systems. The more steps the signal has to go through the more it is susceptible to noise. Analog systems also use more power. The signal can be converted to a digital signal using an analog to digital converter for the microcontroller to perform further tasks.

Digital sensors produce a finite discrete output. The resulting output is in binary digital form consisting of 1s and 0s. The signal measured is directly converted into a digital signal output inside of the digital sensor itself. Digital systems must provide information at a much faster rate than analog systems, since every point of data must be expressed as a series of numbers. While noise and non-ideal transfer functions are not problems for digital systems an important limitation remains in the maximum sampling rate at which data points can be input or output. And while a digital system can handle any desired level of accuracy, processing time and memory size suffer with higher accuracy. Digital systems draw negligible power. Digital sensors communicate with a microcontroller using a communication protocol such as: I2C (Inter-Integrated circuit), SPI (Serial Peripheral Interface) and One Wire. There are other protocols but these are the most common. Using I2C or SPI means I can have arbitrary precision from the sensors.

3.3.1.1 Active vs Passive

To talk about active and passive devices then I need to talk about transducers. An electrical transducer changes energy of one kind to energy of another kind. The output energy is differing in kind but related to the input.

Active transducers generate electric current or voltage directly in response to an environmental change. It also requires an external power supply to operate, called an excitation signal which is used by the sensor to produce an output signal. Passive transducers produce a change in some passive electrical quantity, such as capacitance, resistance, or inductance, as a result of a measured change. They require additional electrical energy for excitation.

3.3.1.2 Additional Factors

It is also important to take into account when choosing a sensor the following things: [2]

1. Sensor Sensitivity

    a. Sensitivity to the measured quantity: If the sensitivity is too high than the sensor may not pick up the desired quantity (whether it’s a vibration or a sound), while if the sensitivity is too low then it will pick up the desired frequency, but it may also be more sensitive to noise.

    b. Insensitivity to other properties: The sensor should have a way to filter out outside signals that are not desired to perform the task for this project

    c. Influence to measured property: While it is looking for a signal, it should not in anyway affect the outcome of that signal. It should only report whether a signal is present or not.

2. Sensor Deviations or “system errors”

    a. The set range: The frequency range matters. Humans can hear anywhere from 20Hz to 20kHz. The range for a cell phone vibration is 151-180Hz. The sensor needs to be able to pick up those frequencies or else they will be outside of the range and the result will be useless.

    b. Sensitivity Error: Using the potentiometer or the microcontroller, the sensitivity desired can be set, however errors can happen in that process. This will be something that will need to be checked when testing begins.

    c. If output signal differs from correct value: If the signal goes though several steps before we see the final result, such as a analog to digital converter, noise along the way may affect the original wave this giving us the wrong output value.

d. Noise: One of the most significant things that can negatively affect this project is noise. Examples of it have been stated above.

e. Temperature in the environment: Heat is a form of kinetic energy just like sound. Molecules at higher temperatures are more excited, they move faster, increasing vibrations which affects sound waves by making them travel faster.

f. Resolution: It is the smallest change in environment that a sensor can detect. This can make a significant difference in what we are trying to do. If it cannot pick up the smallest possible value then it won't work correctly 100% of the time.

3.3.2 Sound Sensors

Sound sensors are used to detect sound in the environment. Sounds are acoustic waves; the sound sensors detect these waves then converts it into an electrical signal to go into a microcontroller. Analog sound sensors consist of the microphone and the board, the microphone picks up the waves, while the board translates the amplitude of the acoustic volume of the sound into an electrical voltage, giving out an analog output. This signal can then be ran into an analog to digital converter for the microcontroller. Meanwhile digital sound sensors already come with an ADC built in, so it can automatically convert it into a digital signal. This is efficient but it also hinders the user from adjusting the sensitivity of the sensors themselves.

3.3.2.1 Microphones

A Microphone is a transducer that changes acoustic waves into electrical signals. The analog output signal (usually a voltage or a current) produced is proportional to the acoustic sound wave acting on the flexible diaphragm. There are several different types of microphones that can be seen below which use different methods of converting the air pressure variations of an acoustic wave into an electrical signal. The three most popular microphones are: condenser, electret condenser, dynamic, mems and piezoelectric.

3.3.2.2 Condenser Microphone

Also called an electrostatic microphone or capacitor microphone (condenser means capacitor) it uses a capacitor to convert acoustical energy into electrical energy. As seen in Figure 1, the microphone has 2 plates, and a battery. When the front plate (the diaphragm) is struck by a sound wave, it moves and that changes the distance between the two plates, thus changing the capacitance. The diaphragm is made of a lighter material for this purpose. It receives power from a battery or an external source.

3.3.2.3 Electret Condenser Microphone

A sub category of condenser microphones. As seen in Figure 13, instead of having an external battery charge it has a permanent charge in an electret material. An electret is a piece of dielectric material that is permanently polarized. This eliminates the need for a polarizing power supply. These are the most widely used microphones today, such as cell phones, computers, headset microphones, etc. It's low material cost and performance make it an ideal choice.

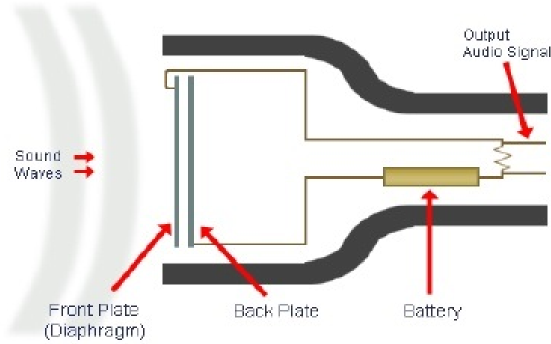


Figure 12 - Condenser Microphone

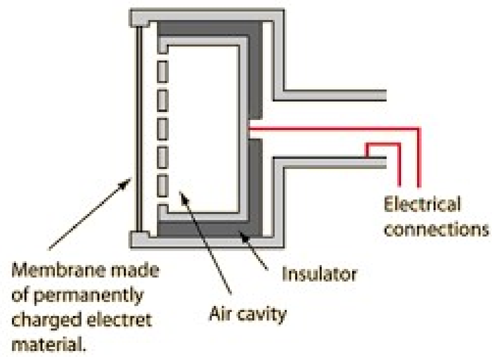


Figure 13 - Electret Condenser Microphone

3.3.2.4 Piezoelectric microphone

Uses piezoelectricity (which is the generation of an electric charge in crystals due to an applied pressure on them) to convert acoustic sound into an electrical signal. As shown in Figure 14, the microphone has a thin layer of piezoelectric material on the diaphragm, when it is hit with an acoustic wave the crystal is deflected. The crystal acquires opposite charges when that happens and the resulting voltage is proportional to how much deformation there was on the crystal due to pressure. The output of the piezoelectric microphones is large, but the high impedance made it easily affected by noise, both from the microphone and the cable.

3.3.2.5

3.3.2.6 Dynamic microphone

As shown in Figure 4, these microphones have a small coil of thin wire hanging within the magnetic field of a magnet. As the sound wave hits the diaphragm, the diaphragm moves begins to vibrate due to the pressure of the wave. As a result, the coil of wire wrapped around the magnet moves within the magnetic field. As the coil moves a voltage is induced in the coil. This is called electromagnetic induction. According to Faraday's Law **Invalid source specified.** "Any change in the magnetic environment of a coil of wire will cause a voltage (emf) to be "induced" in the coil. No matter how the change is produced, the voltage will be generated. The change could be produced by changing the magnetic field strength, moving a magnet toward or away from the coil, moving the coil into or out of the magnetic field, rotating the coil relative to the magnet, etc." Then the resulting output voltage due to the coil is directly proportional to the pressure of the sound wave. Meaning the stronger the sound wave the bigger the output signal will be. Dynamic microphones are preferred in audio studios since they are robust, inexpensive, resistant to moisture, and have a high gain feedback.

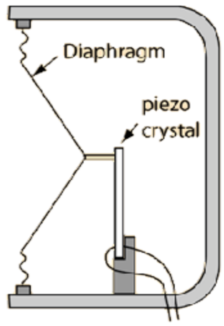


Figure 14 - Piezoelectric microphone

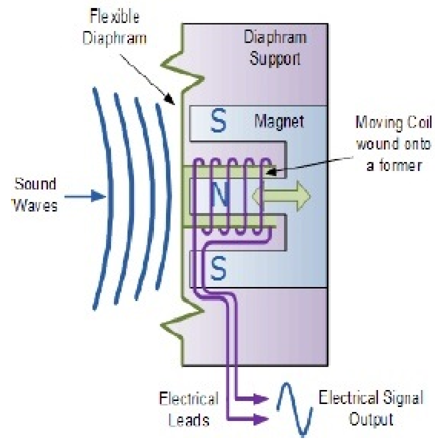


Figure 15 - Dynamic microphone

3.3.2.7 MEMS (Micro Electrical-Mechanical System) Microphone

MEMS technology is enabling microphones to be smaller and available with either analog or digital outputs. The output of a MEMS microphone does not come directly from the MEMS transducer element. The transducer is essentially a variable capacitor with an extremely high output impedance. Inside the microphone, the transducer's signal is sent to a preamplifier, whose first function is an impedance converter to bring the output impedance down to something more usable when the microphone is connected in an audio signal chain. The microphone's output circuitry is also implemented in this preamp. For an analog MEMS microphone, this circuit whose block diagram is shown in Figure 17 is basically an amplifier with a specific output impedance. In a digital MEMS microphone, shown in Figure 16, that amplifier is integrated with an analog-to-digital converter (ADC) to provide a digital output in either a pulse density modulated (PDM) or I^2S format.

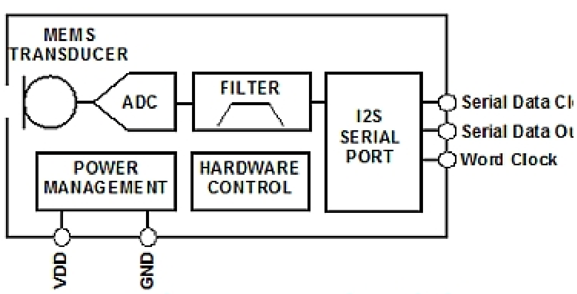


Figure 16 - Digital MEMs microphone

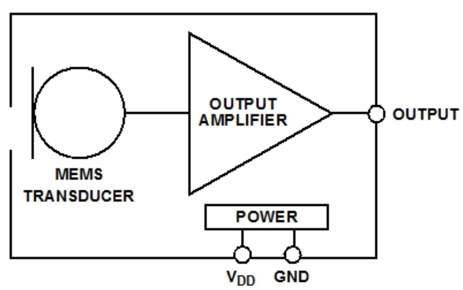


Figure 17 - Analog MEMs microphone

3.3.2.8 Microphone Comparisons

There are a few things to look for when it comes to the microphone desired to pick up the sound. Condenser microphones offer a strong output signal, sensitivity, frequency range and stability than dynamic microphones. Meanwhile dynamic microphones have a better frequency response, robust, inexpensive and have a high gain feedback. Piezoelectric offer a high electrical output. MEMs microphone are analog and digital so depending on what you need done, they may be easier and faster to work with, they are also less affected by noise. However the best microphone for our project seems to be elecret condenser microphones. They are low cost, high performance and already exist in a variety of sound sensors ready to connect to a microcontroller for further signal processing.

3.3.2.9 Polar Patterns

Another factor to consider with a sound sensor is the direction of the microphone. The sound sensor will be placed on the back wall of a box facing the phone. We only want it to detect the sound waves coming from the phone, waves coming from any other direction is negligible. If it is picking up sounds from other directions then they will be unnecessary noise that will affect the outcome of whether the phone has been vibrating, ringing or neither.

Some of the polar patterns available are omni-directional, bi-directional, sub-cardioid, cardioid, hyper-cardioid, super-cardioid, and shotgun as shown in Figure 7. Omni-directional microphones are basically a perfect sphere, it can detect waves in all three dimensions. Bi-directional is shaped like a number 8, where it will look for sound waves in the front and back of the device but not the sides. Uni-directional looks for sounds only in one direction. They are shaped like an apple, where it rejects sounds from the sides and the back. Cardioid, hypercardioid, supercardioid, subcardioid, are all unidirectional microphones. Some microphones also take into account other factors that change its polar pattern. The housing itself, such as the one we have can greatly affect the pattern. If there is no housing then omnidirectional could be ideal, but when there is a housing that forces the sensor to only aim at one direction then cardioid unidirectional could be best.

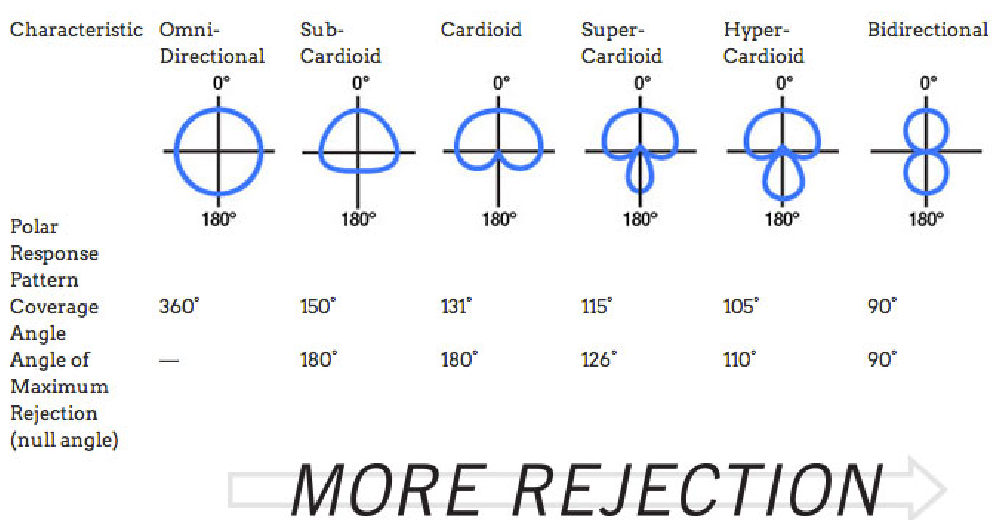


Figure 18 - Polar Patterns

3.3.2.10 Sound Sensor Selection

The table below shows several examples of Electret microphones under consideration since that is the microphone that will be most useful for our project.

Table 4:Sound Sensor Characteristics

Sensor	**Features**
Grove Sound Sensor	Electret microphone
	Omni-directional
	LM358 amplifier
	Analog Output
	Connects to various platforms
Grove Loudness Sensor	Electret microphone
	Omni-directional
	LM2904 amplifier
	Filters high frequency signal, outputs positive envelope
	Input signal filters twice in module to avoid signal disturbances
Phantom Yojo Sound Sensor	Electret microphone
	Omni directional
	LM393 Amplifier
	Outputs analog or digital value
	Stable performance
	AD transform for sound intensity
KY-038 Microphone Sensor	Electret microphone
	Omni-directional
	Outputs analog or digital value
Sparkfun Sound Sensor	Electret microphone
	Omni-directional
	LM324 Amplifier
	Peark detector, buffer amplifier, Schmitt trigger
	Outputs analog or digital value
	Through-hole resistor to adjust threshold

Looking at some characteristics of each sensor is not enough, we must also compare the specifications of each one to determine if it'll work with the equipment that we want to use.

Table 5: Sound Sensors Specifications

	Grove Sound Sensor	**Grove Loudness sensor**	**Phantom Yoyo Sound Sensor**	**KY-038 Microphone Sensor**	**Sparkfun Sound Sensor**
VCC	3.3-5V	3.5-10V	4-5V	5V	3.3V-5.5V
Operating Current (Vcc=5V)	4-5mA	5mA	4mA	5mA	5mA
Sensitivity at 1kHz	52-48dB	48-66dB	46-58dB	44-48dB	40-60dB
Frequency	16-20kHz	50-2kHz	30-5kHz	100-10KHz	20-10kHz
S/N Ratio	54dB	>58dB	56dB	58dB	58dB
Platform Support	Arduino, Wio, Beaglebone, Raspberry Pi, Linkit	Arduino, Wio, Beaglebone, Raspberry Pi, Linkit	Arduino, AVR, ARM	Arduino	Arduino
Potentiometer	Yes	Yes	Yes	Yes	No
Price	$7.99	$9.99	$5.69	$18.58	$11.95

After taking into account the characteristics and specifications of each sensor, we know that we want to use a sensor with an analog output. That way we have the freedom to adjust the sensitivity of the sensor with the potentiometer, and can have our own analog to digital converter of our choice rather than the one built in with digital converters. The sensors which have an analog output are also cheaper even if they are more likely to be distorted by noise. Out of all these options the grove sound sensor seems to be the best choice; seen in Figure 19. It has an analog output, it is cheap, it detects sound in the range that we want it to, it has our ideal microphone and polar pattern, and it has a potentiometer for easy adjustment.

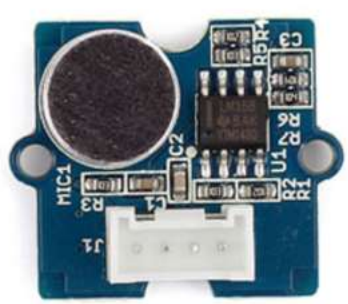


Figure 19 - Grove Sound Sensor

3.3.3 Vibration sensors

Vibration sensors are used to detect vibrations in the environment. There are three categories of vibration sensors: displacement, velocity and acceleration. A variety of sensors, can detect vibration even if they are not technically vibration sensors. Vibration Transducers are more complex sensors that have an output voltage or current.

3.3.3.1 MEMS Accelerometers

Accelerometers are transducers which are designed to measure acceleration forces. They detect change in position, velocity, orientation, shock, vibration and tilt. They measure low to high frequencies and they produce a constant variable voltage based on the amount of acceleration applied to the accelerometer. Micro-electro mechanical systems, they measure frequencies down to 0 Hz (static or DC acceleration). In Figure 9 you can see the structure for a MEMS Accelerometer. PCB manufactures two types of MEMS accelerometers: variable capacitive and piezo-resistive. Variable capacitive (VC) MEMS accelerometers are lower range, high sensitivity devices used for structural monitoring and constant acceleration measurements. Piezo-resistive (PR) MEMS accelerometers are higher range, low sensitivity devices used in shock and blast applications.

3.3.3.2 Piezoelectric Pressure Sensors

These are transducers which senses the pressure as it converts it to an electrical signal. They have high sensitivity when converting sound pressure into voltage. As seen in Figure 10, the sensor turns a mechanical force into an electrical voltage. The piezo electric effect generation of electrical charge in certain crystals due to applied mechanical stress on them. The rate of electrical charge is proportional to the force applied on it. It also works in reverse, if a voltage is applied then it can generate mechanical energy. A quartz crystal is a piezo electric material. It can generate a voltage when mechanical stress is applied on the crystal. The piezoelectric crystal bends in different directions at different frequencies, this is called mode vibration. For different vibration modes, the crystal can be made in different shapes.

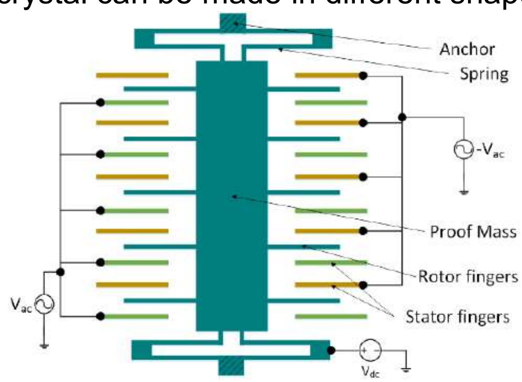


Figure 20 - MEMS Accelerometer Structure

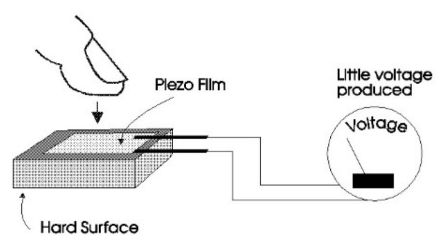


Figure 21 - Piezoelectric Sensor Structure

3.3.3.3 Sensor selection

The table below shows several examples of Accelerometers and Piezoelectric transducers since they are both under consideration for this project.

Table 6: Analog Sensor Characteristics

sensor	features
MiniSense 100 Piezo Vibration Sensor	Piezoelectric Transducer
	Low cost
	High sensitivity at low frequencies
	Higher voltage output
	Analog Output
	Highly receptive to high schock
LDT0-028	Piezoelectric Transducer
	Piezo Film Sensor
	High Sensitivity
	AC coupled
	Robust
Goedrum Piezo Disc	Piezoelectric Transducer
	Clear sound
	Thin and Lightweight
	No noise
	Low power consuption
Triple Axis Accelerometer	Accelerometer
	3 axis sensing
	Small, low profile
	Low power
	Digital Output
	2-3.6V Power supply
	I2C/Acceleration +/-2,4,8,16g
	Compatible with Arduino
ADXL335	Accelerometer
	3 axis sending
	Small, low profile
	Low power
	High resolution
	Analog output

Looking at some characteristics of each sensor is not enough, we must also compare the specifications of each one to determine if it'll work with the equipment that we want to use.

Table 7: Sensor Comparison

Vibration Sensor	**MiniSense100**	**LDT0-028**	**Goedrum Piezo Disc**	**ADXL335**
	Piezo-electric sensor	Piezo-electric sensor	Piezo-electric sensor	Accelerometer
Type	Cantilever-type	Regular	Disc-type	Chip
Resonance Frequency	75Hz	180Hz	1.3Hz +/-0.5kHz	5.5kHz
Voltage Sensitivity	6 V/g	1.4 V/g	4V/g	3V
Operating voltage range	5V	5V	5V	1.8-3.6V
Capacitance	244pF	80pF	40pF	50pF
Price	$4.39	$3.79	$11.90	$6.98

After taking into account the characteristics and specifications of each sensor, we know that we want to use the piezo-electric transducer rather than an accelerometer. They are more sensitive to converting sound pressure to an electrical signal and they are more widely used in the real world for projects similar to ours. The sensors which have an analog output which is what we wanted, since it is cheaper even if they are more likely to be distorted by noise. Out of all these options the mini sense 100 piezo-electric vibration sensor seems to be the best choice; seen in Figure 11. It has an analog output, it is cheap, it is an piezoelectric transducer, it is highly sensitivity at low frequencies, and it has a higher voltage output. Since the phone will be vibrating at a low frequency, this vibration sensor is ideal in our scenario.

Figure 22 - Mini Sense 100 Vibration Sensor

3.3.4 Reed Switch

A Reed switch acts as a position sensor. It can send a signal of when something is either open or closed. This is very handy for our locking mechanism. The switch will be used to tell the microcontroller if the door is closed or not, which will then communicate to the locking mechanisms of whether it should lock the door or not. As seen below, in Figure 1, the way a reed switch works is when you bring a magnet up to a reed switch, the two contacts of the reed switch become opposite magnetic poles, they attract so the two ferrous materials inside the switch pull together and the switch closes. This is called its normally open stage. When the magnetic field is removed, the reeds separate and the switch opens. When you take the magnet away the contacts split apart and return to their original positions. Also it doesn't matter which end of the magnet approaches first, the contacts will polarize in opposite ways and attract each other. The other option is when the switch is normally closed. In this scenario the circuit is closed, say someone leaves their phone in the locker then the door will remain shut until the fingerprint scanner says that It is okay to open, then when you bring a magnet to the switch, the two contacts that are normally snapped together will spring apart. This means that electricity will be flowing through them most of the time. Reed switches in general make a great non-contact switch. This minimizes accidents and increases security.

3.3.4.1 Switch Selection

The table below shows several examples of reed switches under consideration.

Table 8 - Reed Switch Characteristics

Magnetic Switch	Effective for Theft Deterrence One of the only switches with both normally closed contacts Great for pick-ups with sliding rear window
Individual Reed Switch	Normally Open 10W Low Voltage Max Operate time: 0.35s Resonant Frequency: 5000Hz
Reed Switch and Magnet Assembly	Switch/magnet combo For alarm systems and door annunciators ½" switch distance to prevent false alarms Versatile Both normally open or normally closed wiring option Up to 125V/0.5A
30-10071 N.O/N.C Magnetic Reed Switch	SPDT magnetic switch/reed switch Alarm contact 0.5A, 20V, 10W max

Figure 23 - Reed Switch

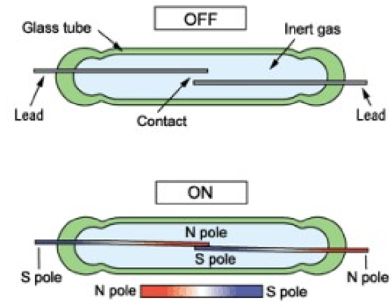


Figure 24 - Reed Switch Functionality

Several reed switches in the market are either normally open or normally closed but not both. The one necessary for this project is the third option Reed Switch and Magnet Assembly combo. It offers both options for N/O and N/C but it also seems to be high quality. It claims that it does not break as quickly or easily as other switches. It goes up to a high available voltage so we don't have to worry about it. A ½" distance to prevent false alarms is very useful, we don't need the device to be randomly opening or closing due to a false alarm. It specifically says that it is used for door enunciators, and we are using this for a door so this is a good choice for the sensor that we use.

3.3.4.2

3.3.5 Sensor Microcontroller Selection

When selecting which microcontroller we will be using to handle the security authorization and authentication, we need to account for all the signals voltage and current requirements of the parts that are to be controlled. We also need to consider the communication that we will be using, which based on the needs of the fingerprint sensor we will will need UART communication. Below we will cover the top options that we could find as well as the benefits and cost of each. We will then decide which one best suites our needs.

3.3.5.1 TI MSP43x Series Microcontroller

Texas Instruments is a well know technology manufacturer that produces a large range of products that that produces and one of the world leaders in produces of microelectronic components. The main serious of low power microcontrollers that Texas Instruments offers are those of the mixed signal processors in the MSP430 and MSP432 family. These microcontrollers offer ultra-low power high performance with a standardized advanced reduced instruction set computer machine (ARM). The MSP430 series operate on a 16-bit platform whereas the msp432 series run on a 32-bit platform. Texas instruments offer a vast amount of components designed specifically to work with the MSP43x families.

3.3.5.1.1 MSP430FG4618

The Texas Instruments microcontroller which we have the most experience for is the MS430FG4618. This was the first option we decided to research since it is used extensively in our undergraduate classes and we all have at least a basic understand of the many capabilities as well as the limitations of it. The key features of this microcontroller are that it runs at 8MHz, it has 80 general purpose input pins, twelve 12-bit analog to digital channels, 116 kB of nonvolatile memory, 8 kB of RAM, 2 built in 16 bit timers, built in comparators, and has the ability to communicate over UART, SPI, and I2C. This has more than we need and should be perfectly capable of handling the security authentication controls but it may be overkill more than we need. We will compare it to our other options.

3.3.5.1.2 MSP430G2553

The second Texas Instruments microcontroller we will consider is the MSP430G2553 which is the microcontroller that comes in the Texas Instruments MSPEXP430G2 LaunchPad. The launch pad this comes in is relatively cheap and some of us have bought it to be able build and test circuits at home as part of extra coding practice, applying the same principles from our undergraduate courses to learning how the differences between the microcontrollers affect coding which was used to enforce good coding practices. This uses the same CPU core as the MSP430FG4618 meaning it also runs the 16-bit architecture but it differs on some of the key features. The key features of this microcontroller are that it runs at 16MHz, it has 24 general purpose input pins, eight 10-bit analog to digital channels, 16 kB of nonvolatile memory, .5 kB of RAM, 2 built in 16 bit timers, built in comparators, and has the ability to communicate over UART, SPI, and I2C. This is a smaller version of the previous microcontroller with a smaller number of pins which would still be enough to handle the needs of our security authentication and lock actuation controls.

3.3.5.1.3 MSP432P401R & MSP432P401M

These Texas Instruments microcontrollers combine the low power efficiency of the of the MSP430's with advanced mixed signal features the high performance processing capabilities of the 32-bit Cortex-M4F RISC engine. Combined with the lightning fast speeds flash memory which allows for simultaneous read and write, these microcontrollers are excellent for data processing and enhanced handling of mixed-signals. The main difference between these two is that the MSP432P104R has more memory all around. Whereas the R has 256 kB of nonvolatile memory and 64 kB of RAM, the M only has 128 kB of nonvolatile memory and 32 kB of RAM. They both run at 16MHz, and they have 24 general purpose input pins, eight 10-bit analog to digital channels, 2 built in 16 bit timers, built in comparators, and have the ability to communicate over UART, SPI, and I2C. Since our design doesn't require heavy processing the 32-bit architecture doesn't add much benefit over the 16-bit architecture found in the regular MSP430xx microcontrollers.

3.3.5.2 Atmel Microcontrollers

Atmel is the other major microcontroller manufacturer that we will be looking into. They have a very broad list of microcontrollers that generally fall into two major groups. There is the ATmega-xx controllers as well as the ATtiny-xx microcontrollers. The main difference between these two categories is the size. The ATtiny-xx microcontrollers are quite small and have significantly less memory and pins than the ATmega-xx microcontrollers. We will look at options of each type for comparison to the microcontrollers offered by Texas Instruments.

3.3.5.2.1 ATtiny25

The ATtiny25 is a low power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATtiny25 achieves throughputs approaching a million instructions per second per MHz. allowing us to optimize power consumption versus processing speed. The key features of this microcontroller are that it can run up to 20 MHz, it has 6 general purpose input pins, four 10-bit analog to digital channels, 2 kB of nonvolatile memory, 128 bytes of RAM, 2 built in 8-bit timers, a built in analog comparator, and has the ability to communicate over SPI and I2C.

3.3.5.2.2 ATtiny417

The ATtiny417 has more to offer than the bare bones of the ATtiny25. It is also low power 8-bit microcontroller with the AVR CPU but it also comes with with a hardware multiplier. The key features of this microcontroller are that it can run up to 20 MHz, it also has 6 general purpose input pins, four 10-bit analog to digital channels, but comes with 4 kB of nonvolatile memory, 256 bytes of RAM, 2 built in 16 bit timers, a built in analog comparator, and has the ability to communicate over USART as well as SPI and I2C.

3.3.5.2.3 ATmega328

The ATmega328 is a high performance low power CMOS 8-bit microcontroller that also uses the AVR CPU. We chose to consider this microcontroller because it is the microcontroller behind most of the arduino microcontroller boards which are widely used and well documented. The key features of this microcontroller are that it can run up to 20 MHz, it has 23 general purpose input pins, eight 10-bit analog to digital channels, 32 kB of nonvolatile memory, 2 kB of RAM, 2 built in 8-bit timers and a 16-bit timer, a built in analog comparator, and has the ability to communicate over USART, SPI and I2C.

3.3.5.3 Microcontroller Comparison and Selection

In choosing which controller we should go with, there are several minimum requirements we must meet. We should try to minimize the power requirement and we need to ensure that we have a UART for communicating with the terminal communication controller. We also need to be able to compare analog inputs for the microphones for rejection of false positives as well as have enough general purpose pins as well as ADC channels as necessary to do the following:

- Take input from 2 microphones
- Take input from vibration sensor
- Take input from locking controller
- Output to status lights

Based on these requirements and the specifications of the considered microcontrollers in Table 9 – Sensing Microcontroller Comparisons, we have chosen to go with the ATmega328. It meets of our requirements for pins, comparators, and has a lower power requirement than the options from Texas Instruments.

Table 9 – Sensing Microcontroller Comparisons

	MSP430G2553	**MSP430FG4618**	**MSP432401R**	**MSP432401M**	**ATMEGA328**	**ATtiny25**	**ATtiny417**
CPU	MSP430	MSP430	ARM Cortex - M4F	ARM Cortex - M4F	AVR	AVR	AVR
Frequency (MHz)	16	8	48	48	20	20	20
Non-volatile Memory (KB)	16	116	256	128	32	2	4
RAM (B)	512	8k	64k	32k	2k	128	256
GPIO Pins (#)	25	80	84	84	23	6	6
I2C	1	1	4	4	1	1	1
SPI	2	1	8	8	2	1	1
UART	1	1	4	4	1	0	1
DMA	0	3	8	8	0	0	0
Analog Digital Converter	ADC10	ADC12	ADC14	ADC14	ADC10	ADC10	ADC10
ADC Channels	8	12	24	24	8	4	4
Comparators (Inputs)	8	8	8	8	1	1	1
Timers - 8-bit	0	0	0	0	2	2	1
Timers - 16-bit	2	2	4	4	1	0	2
Timers - 32-bit	0	0	2	2	0	0	0
Boot Strap Loader	UART	UART	UART/I2C/SPI	UART/I2C/SPI	UART/I2C/SPI	I2C/SPI	UART/I2C/SPI
Min VCC	1.8	1.8	1.8	1.8	1.8	1.8	1.8
Max VCC	3.6	3.6	3.6	3.6	5.5	5.5	5.5
Active Power (uA/MHz)	330	400	400	400	200	200	200
Standby Power (uA)	0.7	1.3	1.3	1.3	0.75	0.75	0.75
Wakeup Time (us)	1.5	13	13	13	60	60	60

3.4 Security

In places of high security, chances are that the people leaving their phones behind are going to want their phones to be secured as well. This section will cover the security measures that we intend to implement in our design.

3.4.1 Locking Mechanisms

The enclosures that will be built in our design require a locking mechanism to securely store the mobile devices. There are many different types of locking mechanisms and based on our needs to be able to control it electronically, our selection has been narrowed down to three different potential types of electric locks for our design.

3.4.1.1 Electromagnetic Door Lock

Electromagnetic door locks are typically mounted to a frame and use a constant DC voltage to induce a current that creates electromagnetic field. This electromagnetic field magnetically bonds the frame with a metal plate that is affixed to the door effectively locking the door shut. These can be controlled by breaking the current to the lock to release the metal plate. Electromagnetic locks are very strong but require a constant power source.[3]

3.4.1.2 Linear Solenoid Actuator Lock

Linear solenoids are devices that convert electric energy into a mechanical motion to pull in a ferromagnetic pin when a voltage is applied. The pin is pulled in by the magnetic field created by the current in the coil of the solenoid. When the voltage is removed, the magnetic field goes away and a spring is used to push the pin back out. Linear solenoids are relatively simple, and have a low power requirement as they only need power to hold open the mechanism.[4]

3.4.1.3 Motorized Electric Latches

Motorized electric latches use an electric motor to rotate a locking mechanism into place. This is a simple design that can use rotary limit control to rotate a latch into a locked or unlocked state. It only needs power when the motor is active. This also allows for a manual override if power is lost.

3.4.1.4 Linear Solenoid Latch

Similar to the linear solenoid pin, solenoid latches create a mechanical motion by using current to pull in a ferromagnetic pin when a voltage is applied. The difference is that it requires only a pulse of current to pull in the pin, then the pin latches to a fixed permanent magnet pole. When a reverse current pulse is sent the magnetic flux of the permanent magnet is effectively canceled out, allowing a spring to push the pin back out. This reduces the power requirement compared to the linear solenoid actuator. For clarity, the functionality of a linear solenoid latch is shown in Figure 25, courtesy of TLX Technologies[5].

3.4.1.5 Mechanism Selection

Based on the pros and cons in Table 10, as well as our needs, the mechanism for our design will be a linear solenoid latch. This will allow for a secure low profile design with low cost that will be power efficient, easy to implement, and long lasting. While it is not very heavy duty, this should not be an issue since the containers themselves will be in a reasonably secure area. Since the default position will be normally closed in the locked position, only unlocking when there is a signal, we will have a battery backup for the controller to allow unlocking during a power outage.

Table 10 - Locking Mechanism Type Comparison

Locking Mechanism Type	**Pros**	**Cons**
Electromagnetic	Can work with any electrical signaling method	Requires Constant Power
	Can withstand a great amount of force.	Can be overcome by disrupting power source
	Strength can be increased by increasing current.	Door could be pried open if framing is weak.
	Tamper resistant	Expensive
		Large in size
		Requires a ferromagnetic material to secure to
Linear Solenoid Bolt	Easy to implement electrically	Not very heavy duty.
	Simple to install	Locked out if power is lost
	Low power requirement	Requires constant current until the door is opened.
	Inexpensive	
	Allows long battery life	
	Small in size	
Motorized Electric Latches	Only requires power when the state is being changed	Large in size
	Allows for a manual keyed override	Many moving parts that require precise alignment
	Allows long battery life	Mid range in price
Linear Solenoid Latch	Simple to install	Can be locked out if building power is lost.
	Very power efficient	
	Inexpensive	
	Most efficient when pulse time is short compared to hold time	

3.4.1.6 Product Comparison and Selection

When choosing a our locking product our main focus was to find a product with a low profile that that used a standard DC voltage and has a low current requirement. The majority of the locks all had the same stroke length so that wasn't an issue. From Table 11 below, we have chosen to go with the Ultra-Compact New Cabinet Door Solenoid Electric Lock Assembly from the distributor ATOPS as it had the least current draw as well as the smallest footprint of those that we compared.

Table 11 - Product Comparison

Product	Voltage DC (Volts)	Current (Amps)	Dimensions (cm)	Stroke Length	Price
Uxcell Open Frame Type Solenoid for Electric Door Lock	12	1.3	6.6 x 4.2 x 3	10mm	$16.14
Uxcell 10mm Stroke Force Open Frame Type Solenoid for Electric Door Lock	12	1.0	6.4 x 2.6 x 2	10mm	$9.92
Amico 0837L Open Frame Type Solenoid for Electric Door Lock	12	0.6	6.6 x 4.0 x 2.7	10mm	$6.21
ATOPS Ultra-Compact New Cabinet Door Solenoid Electric Lock Assembly	12	.35	2.7 x 2.9 x 1.8	10mm	$4.75
UHPPOTE File Display Cabinet Drawer Latch Assembly Solenoid Electric Lock	12	.6	5.45 x 4.1 x 2.8	10mm	$12.50

Figure 25 below, shows the functionality of the linear solenoid latch that we have decided to use in our design.

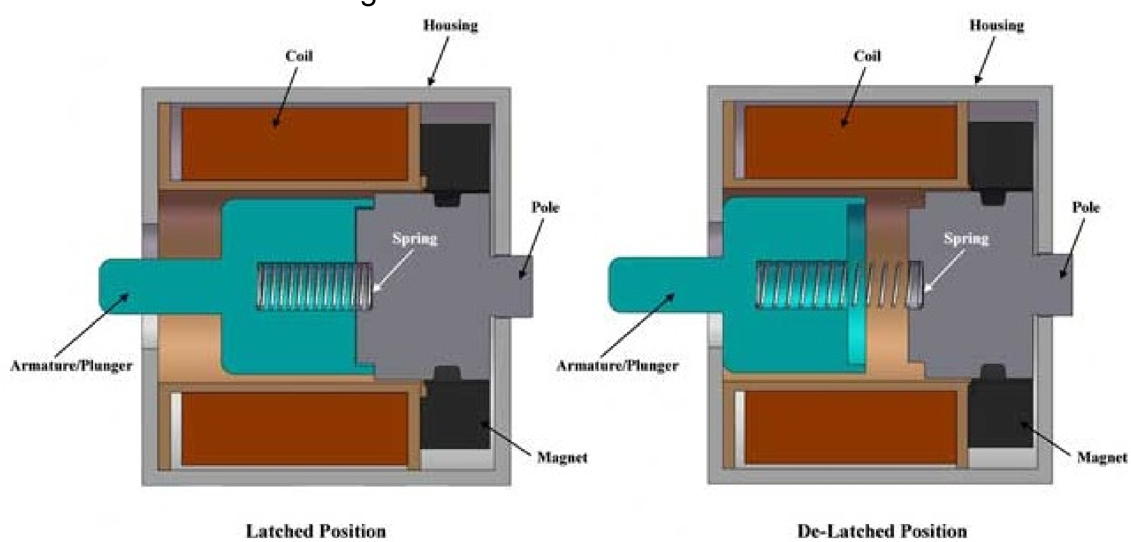


Figure 25 - Linear Solenoid Latch Functionality

3.4.2 Authentication Method

Authentication is the processes by which we confirm and verify the truth of an attribute. In our case, we need to verify the identity of the person attempting to gain access to one of the lockers in which a phone is being stored. There are three major categories of authentication; something you know, something you have, and something you are.

Something you know would be a something like a shared secret, usually a password, phrase or gesture. It is typically the least secure of the three major categories as many people are complacent and don't take care to ensure someone else isn't watching listening to copy the 'secret'. Many people also often use easy, or simple to guess passwords also which adds to the insecurity of this category further.

Something you have would be a security token, key, key card, or some other physical device that you carry on your persons. There are typically quite secure depending on how hard it is to duplicate. Something you have is most often used in 2-factor authentication in conjunction with a password or pin for added security.

Something you are would be something that is part of you which is usually very hard to replicate and is typically the most secure. The most common form of something you are comes in the form of biometrics such as fingerprint scans, retinal scans, hand print or voice print. The implementation of biometrics is significantly more elaborate than the other 2 categories and though it is sometimes used in 2-factor authentication, it is complex and secure enough to be a standalone authentication. An elaboration of the authentication methods under consideration can be found below.

3.4.2.1 Integrated Circuit Card

An integrated circuit card (ICC), sometimes known as a smart card, refers to any wallet sized card that has an integrated circuit embedded in it. This falls under that They are typically made of plastic but occasionally other materials are used. ICC's can be either contact or contactless. They can provide a strong security authentication for single sign-on (SSO) within companies and organizations and have a variety of uses. The largest and most widespread implementation of this technology is Europay MasterCard Visa (EMV)-compliant cards which are used worldwide.

Integrated Circuit card can be contact, contactless or a hybrid of the two. Contact ICC's are made up of multiple gold plated contact pads which are used as a medium to communicate when inserted into a card reader. The card reader also functions as the power source for the card through these contacts also. While the specific shape of the contacts can vary, the functionality, communication protocols, physical and electrical characteristics all typically comply with ISO/IEC

7810 [6] and ISO/IEC 7816[7]. In **Error! Reference source not found.**, you can see an example of a generic pin out for an ICC. In Contactless ICC technology, the cards only require a close proximity to an antenna to be able to be powered and communicate through RF induction technology.

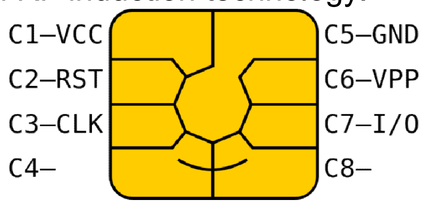


Figure 26 - Generic ICC Pinout

The type of ICC that would best suit our design would be identification ICC's which are becoming increasingly more popular around the world as the technology becomes easier to manufacture. The identification ICC comes in several different implementation methods. Some large scale operations incorporate a public key infrastructure (PKI) such as the Department of Defense's Common Access Card [8] which is the standard identification for all active duty, uniformed service personnel, Selected Reserve, DoD civilian employees as well as government contracted personnel. This has the potential to be an effective authentication method as we could use a card reader which could be more stable and have a lower power requirement than some other methods. The downside would be the potential for losing the card.

3.4.2.2 Numeric Keypad

Numeric keypads could A keypad is simply a surface with buttons that bear numbers, alphabetical letters, symbols or a combination of these. In a security sense, they can be used to enter memorized words, phrases, numeric combinations or otherwise some form of "password." The most generic form of a keypad is a numeric keypad which can be found on keyboards, ATMs, telephones etc. Many devices follow the standard E.161 set by International Telecommunication Union[9] which details the "Arrangement of digits, letters and symbols on telephones and other devices that can be used for gaining access to a telephone network."

A numeric keypad would be the best keypad that we could be used for our design. It would be relatively easy to implement electronically with the use of multiplexers and decoders to reduce the number of processor pins that would be needed as well as inexpensive. Potential downsides with a keypad for authentication would be if people forget their password, have their password compromised and the potential size of keypad as there is a limited amount of space that we have for the authentication design.

3.4.2.3 Near Field Communication Token

Near-field communication (NFC) is a short range, low power communication protocol that enables two electronic devices to establish communication by bringing them typically within range of roughly 10cm from one another. The two devices create a high frequency magnetic field between the loosely coupled coils in both the initiating device and the NFC tag. An NFC tag is a small device with an antenna and a microchip as shown in Figure 27 courtesy of Ubitap [10]. Once this field is established, a connection is formed and information can be passed between the initiator and the tag. The way the communication is established is the initiator sends a message to the tag to find out what type of communication the tag uses. There are 3 types of communication that can be used. NFC-A, NFC-B, and NFC-F. RF Wireless World [11] describes the differences between these. The signaling type NFC-A is based on ISO/IEC 14443A [12]. In the type-A based communication, a delay encoding, also known as miller encoding, technique is employed along with AM modulation. Binary data is transmitted with the data rate of roughly 106 Kbps using type A communication. The binary signal must change from 0 % to 100 % to distinguish between binary 1 and binary 0 data. With NFC-B, the communication is based on ISO/IEC 14443B. This uses Manchester encoding technique [13] which is a special case of binary phase-shift keying (BPSK), where the data controls the phase of a square wave carrier whose frequency is the data rate. With NFC-B, AM modulation at 10% is used rather than the 100% that is used with type A. This convention is used to distinguish between binary 1 and 0. 10% change from 90% for binary 0 and 100% for binary 1 is used. NFC-F is based on FeliCa[11], which is a faster form of RFID communication that is mostly used in Japan for various applications such as credit or debit card based payments, subway, or personal identification.

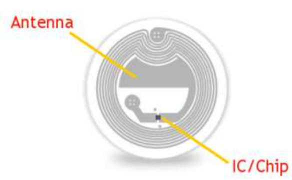


Figure 27 - NFC Tag

According to NFC Forum [14], there are multiple types of tags that are commercially available and are based on existing contactless products. The standard ISO/IEC 14443A[15] details tag types 1,2, and 4 while type 3 is covered by the Japanese standard (JIS) X 6319-4. Type 1 tags are tags that are read and re-write capable and users can configure the tag to become read-only. The memory available in type 1 is 96 bytes and expandable to 2 kilobytes. Type 2 tags are read and re-write capable as well. Users can also configure these tags to become read-only. The difference is that the memory available is 48 bytes and expandable to 2 kilobytes. Type 3 tags are pre-configured by the manufacture to be either read and re-writable, or read-only. Though the memory availability for type 3 varies, the theoretical memory limit is 1MB per service. Last is type 4 which is pre-configured by the manufacturer to be either read and re-writable, or read-only. The memory availability is variable, up to 32 KBytes per service; the communication interface is either Type A or Type B compliant. Once the tag responds the initiators message with the communication type and tag type, the initiator sends its first commands in the appropriate specification. The tag receives the instruction and checks if it is valid. If the instruction is invalid, nothing occurs. If it is a valid request, the tag then responds with the requested information. For sensitive transactions such as credit card payments, a secure communication channel is first established and all information sent is encrypted. NFC tags function at half duplex while the initiator functions at full duplex. Half duplex refers to a device that can only send or receive, but not both at once. Full duplex can do both simultaneously. A NFC tag can only receive or send a signal, while the interrogating device can receive a signal at the same time it sends a command. Commands are transmitted from the initiator using phase jitter modulation (PJM) to modify the surrounding field and send out a signal. The tag answers using inductive coupling by sending a charge through the coils in it. Meeting theses specifications ensures all NFC devices and tags can communicate effectively with one another [10]. For our design NFC would be relatively secure, but has some of the same implementation issues as integrated circuit cards.

3.4.2.4 Fingerprint Scanner

Because fingerprint recognition, like most biometrics, has a lot of non-trivial information in the physical layer, it is important to understand how we recognize fingerprints, scientifically, before we consider sensors, their accuracy, and their practicality for our design. To begin, biometrics refer to a person's physical characteristics, specifically the measurements associated with how a person looks or moves. Authentication using biometrics is a strong form of security that is used in a large range of applications. There are physical biometrics and behavioral biometrics. Some of the forms of physical biometrics used in security applications include retinal scans, fingerprint scans, palm scans, or hand and finger geometry or facial recognition. Behavioral would include keystroke or typing recognition or analyzing a person's gait. Voice recognition falls into both as it depends on physical characteristics as well as the specific inflections a person uses. Fingerprint recognition is by far the least expensive, most common and widely used form of biometrics which is why we will consider it for our design.

3.4.2.4.1 Physical Layer Background

General Fingerprint Patterns: Like the category of topology, we will not be going extensively into specific types, such as tented arches [16], but general categories such as arches, loops and whorls. According to Biometric Solutions [17], arches as shown in Figure 28, generally start at a side, buckle in the center and terminate at the other side of the finger. Loops, as shown in Figure 29, generally start at one side, form a loop around some focus, and then terminate back at the same side of the finger. Whorls, as shown in Figure 30, are generally concentric patterns around central points.

Figure 28 – Arch

Figure 29 – Loop

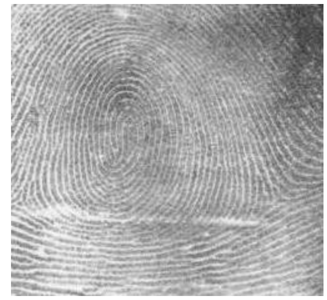


Figure 30 - Whorl

Identifying features (Minutiae features):

Figure 31 - Ridge Ending

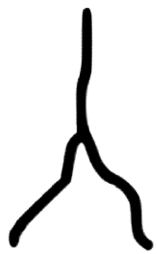


Figure 32 – Bifurcation

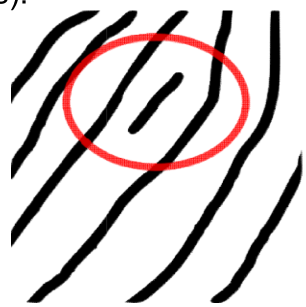


Figure 33 - Short Ridge/Dot

As biometric solutions points out, there are two types of fingerprint matching, which in our case will be digitizing, there is minutiae matching, and pattern matching. In minutiae matching, it simply digitizing the information regarding the Dots, Ridge-Ending points and Bifurcation points, and compares those. In Pattern matching, it compares the images directly for similarity.

The most common readers used for detecting fingerprints are optical, capacitive, ultrasound, and thermal readers. Optical Sensors are typically the cheapest, but fall short in actual optical detection, which means that patterns are very easy to replicate. These have also been around the longest when it comes to available scanners. The way an optical scanner works is shines a light source such as an LED that then reflects off of a skin contact point back to a sensor, typically a charge-coupled device (CCD) or a complementary metal-oxide semiconductor (CMOS)[18]. Thermal readers are the same as optical, except they commonly use infrared to detect the heat of a fingerprint. There have been some noted concerns of reliability and environmental temperatures. [18] It has also been noted to need to act fast as heat will try to equalize, and with very small heat differences to begin with, that equilibrium will take effect very quickly. This may also cause problems with rescans, as one would have to wait for the temperatures to settle a second time. Capacitive fingerprint scanners, instead of trying to create a traditional image of a fingerprint, actually use complex integrated circuits with many different small capacitive plate to detect the capacitance which differs between finger ridges and finger valleys. [18] [19] These types of sensors are generally harder to bypass, as it requires a physical object and material with similar properties to the fingerprint itself, and not just an optical blockade similar to the fingerprint. These tend to be a bit more expensive. These tend to be a happy medium that many consumer grade products, such as flagship smart phones, use. Ultrasound Sensors are one of the latest designs in fingerprint scanners. They are typically fairly expensive, and reserved for higher end security platforms in which security and reliability is the largest concern. Currently there are very few ultrasonic fingerprint sensors on the market.

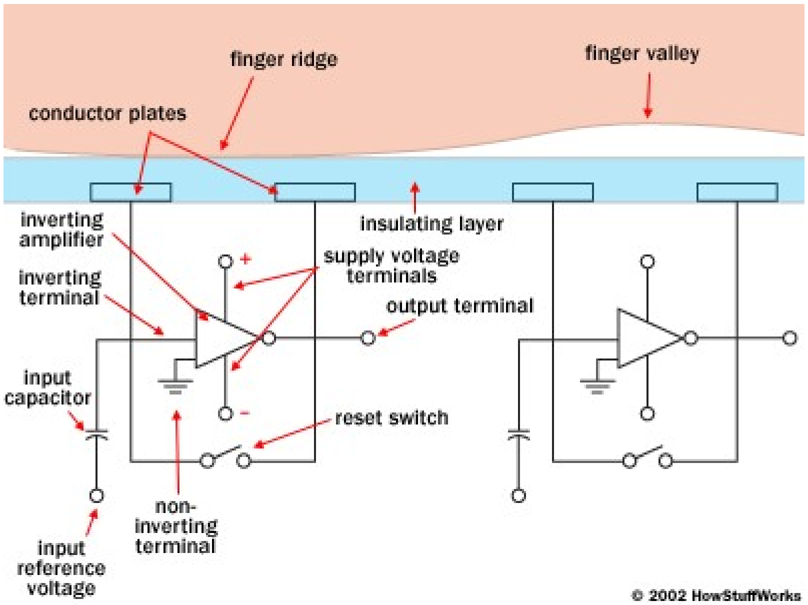


Figure 34 - Capacitive Fingerprint Scanner

Decision: Capacitive fingerprint scanner would be optimal if the price-range is reasonable.

3.4.2.4.2 Storage

There are ANSI/NIST standards for the storage of biometric data. ANSI/NIST-ITL 1-2000 applies to the data formatting and transmission of Fingerprint, Facial, Scar Mark, and Tattoo information. [19] These will be covered in the standards and constraints in 6.6.2.1.

3.4.2.5 Authentication Method Selection

Based on the pros and cons in Table 12, as well as our needs and preferences for our design, the authentication method for our design will be a fingerprint scanner. This will allow for the most secure method of authentication since it cannot be stolen or replicated easily. It will also provide an ease of access since there is no password memorization and no chance you will lose your fingerprint. While the average cost is slightly more than the other methods, it is worth it from a security standpoint.

Table 12 - Authentication Method Selection

Authentication Method	**Pros**	**Cons**
Integrated Circuit Card	Low power requirement	Card can be misplaced, lost, or stolen
	Can incorporate existing company ID's if they are already being used within facility	should be implemented as part of 2-factor authentication instead of stand alone
	Inexpensive to implement	
	Can share access if desired	
Numeric Keypad	Low power requirement	Requires memorization of a pass code
	easy implementation	vulnerable to eavesdropping
	Inexpensive to implement	can take up a significant amount of space
Near Field Communication	Very compact implementation	NFC tag can be misplaced, lost, or stolen
	More secure than numeric keypad	Should be implemented as part of 2-factor authentication instead of stand alone
	Low power requirement	Depending on the sensitivity of the facility, it may not be allowed in facility either.
	Can share access if desired	
Fingerprint Scanner	Highly secure	Unable to share access
	Zero chance of losing or misplacing your fingerprint	more expensive than other methods
	Does not require memorization of a password	
	Difficult to replicate or fool	

3.4.2.6 Product Comparison and Selection

When choosing a specific fingerprint scanner, our main focus was to find a device which would be compatible with our controller as well as low cost. In the decision making process we looked at four possible sensors, two that were capacitive and two that were optical. We compared the communication format, the resolution in dots per inch, the voltage and operating current and as well as the number of fingerprints that could be stored within the scanner. Based on these comparisons, which were tabulated as shown in

Table 13, we have chosen to go with the R303 fingerprint scanner for our prototyping purposes. We expect it work well but because the cost is somewhat high, we want to prototype and test one in a circuit before make a full order. The communication type is UART which means that we will need tom make certain that the microcontroller that it will be tied to has UART communication capabilities.

Table 13 - Fingerprint Scanner Comparison

Fingerprint Scanner	**GT-511C1R**	**R303**	**R306**	**EM406**
Communication	UART	UART	UART	UART
Type	Optical	Capacitance	Capacitance	Optical
Manufacturer	ADH-Tech	Grow	Grow	HFSecurity
resolution(dpi)	450	508	363	508
Price	$31.95	$28.00	$38.00	$42.99
Operating Current(mA)	<100	<55	<60	<100
Fingerprint Storage #	20	1000	1000	1000
Voltage (V)	5	5	5	5

3.4.3 Security Microcontroller

When selecting which microcontroller we will be using to handle the security authorization and authentication, we need to account for all the signals voltage and current requirements of the parts that are to be controlled. We also need to consider the communication that we will be using, which based on the needs of the fingerprint sensor we will will need UART communication. Below we will cover the top options that we could find as well as the benefits and cost of each. We will then decide which one best suites our needs.

3.4.3.1 TI MSP43x Series Microcontroller

Texas Instruments is a well know technology manufacturer that produces a large range of products that that produces and one of the world leaders in produces of microelectronic components. The main serious of low power microcontrollers that Texas Instruments offers are those of the mixed signal processors in the MSP430 and MSP432 family. These microcontrollers offer ultra-low power high performance with a standardized advanced reduced instruction set computer machine (ARM). The MSP430 series operate on a 16-bit platform whereas the msp432 series run on a 32-bit platform. Texas instruments offer a vast amount of components designed specifically to work with the MSP43x families.

3.4.3.1.1 MSP430FG4618

The Texas Instruments microcontroller which we have the most experience for is the MS430FG4618. This was the first option we decided to research since it is used extensively in our undergraduate classes and we all have at least a basic understand of the many capabilities as well as the limitations of it. The key features of this microcontroller are that it runs at 8MHz, it has 80 general purpose input pins, twelve 12-bit analog to digital channels, 116 kB of nonvolatile memory, 8 kB of RAM, 2 built in 16 bit timers, built in comparators, and has the ability to communicate over UART, SPI, and I2C. This has more than we need and should be perfectly capable of handling the security authentication controls but it may be overkill more than we need. We will compare it to our other options.

3.4.3.1.2 MSP430G2553

The second Texas Instruments microcontroller we will consider is the MSP430G2553 which is the microcontroller that comes in the Texas Instruments MSPEXP430G2 LaunchPad. The launch pad this comes in is relatively cheap and some of us have bought it to be able build and test circuits at home as part of extra coding practice, applying the same principles from our undergraduate courses to learning how the differences between the microcontrollers affect coding which was used to enforce good coding practices. This uses the same CPU core as the MSP430FG4618 meaning it also runs the 16-bit architecture but it differs on some of the key features. The key features of this microcontroller are that it runs at 16MHz, it has 24 general purpose input pins, eight 10-bit analog to digital channels, 16 kB of nonvolatile memory, .5 kB of RAM, 2 built in 16 bit timers, built in comparators, and has the ability to communicate over UART, SPI, and I2C. This is a smaller version of the previous microcontroller with a smaller number of pins which would still be enough to handle the needs of our security authentication and lock actuation controls.

3.4.3.1.3 MSP432P401R & MSP432P401M

These Texas Instruments microcontrollers combine the low power efficiency of the of the MSP430's with advanced mixed signal features the high performance processing capabilities of the 32-bit Cortex-M4F RISC engine. Combined with the lightning fast speeds flash memory which allows for simultaneous read and write, these microcontrollers are excellent for data processing and enhanced handling of mixed-signals. The main difference between these two is that the MSP432P104R has more memory all around. Whereas the R has 256 kB of nonvolatile memory and 64 kB of RAM, the M only has 128 kB of nonvolatile memory and 32 kB of RAM. They both run at 16MHz, and they have 24 general purpose input pins, eight 10-bit analog to digital channels, 2 built in 16 bit timers, built in comparators, and have the ability to communicate over UART, SPI, and I2C. Since our design doesn't require heavy processing the 32-bit architecture doesn't add much benefit over the 16-bit architecture found in the regular MSP430xx microcontrollers.

3.4.3.2 Atmel Microcontrollers

Atmel is the other major microcontroller manufacturer that we will be looking into. They have a very broad list of microcontrollers that generally fall into two major groups. There is the ATmega-xx controllers as well as the ATtiny-xx microcontrollers. The main difference between these two categories is the size. The ATtiny-xx microcontrollers are quite small and have significantly less memory and pins than the ATmega-xx microcontrollers. We will look at options of each type for comparison to the microcontrollers offered by Texas Instruments.

3.4.3.2.1 ATtiny25

The ATtiny25 is a low power CMOS 8-bit microcontroller based on the AVR enhanced RISC architecture. By executing powerful instructions in a single clock cycle, the ATtiny25 achieves throughputs approaching a million instructions per second per MHz. allowing us to optimize power consumption versus processing speed. The key features of this microcontroller are that it can run up to 20 MHz, it has 6 general purpose input pins, four 10-bit analog to digital channels, 2 kB of nonvolatile memory, 128 bytes of RAM, 2 built in 8-bit timers, a built in analog comparator, and has the ability to communicate over SPI and I2C.

3.4.3.2.2 ATtiny417

The ATtiny417 has more to offer than the bare bones of the ATtiny25. It is also low power 8-bit microcontroller with the AVR CPU but it also comes with with a hardware multiplier. The key features of this microcontroller are that it can run up to 20 MHz, it also has 6 general purpose input pins, four 10-bit analog to digital channels, but comes with 4 kB of nonvolatile memory, 256 bytes of RAM, 2 built in 16 bit timers, a built in analog comparator, and has the ability to communicate over USART as well as SPI and I2C.

3.4.3.2.3 ATmega328

The ATmega328 is a high performance low power CMOS 8-bit microcontroller that also uses the AVR CPU. We chose to consider this microcontroller because it is the microcontroller behind most of the arduino microcontroller boards which are widely used and well documented. The key features of this microcontroller are that it can run up to 20 MHz, it has 23 general purpose input pins, eight 10-bit analog to digital channels, 32 kB of nonvolatile memory, 2 kB of RAM, 2 built in 8-bit timers and a 16-bit timer, a built in analog comparator, and has the ability to communicate over USART, SPI and I2C.

3.4.3.3 Microcontroller Comparison and Selection

In choosing which controller we should go with, there are several minimum requirements we must meet. We should try to minimize the power requirement and we need to ensure that we have a UART for communicating with the fingerprint sensor and enough general purpose pins as well as ADC channels as necessary to do the following:

- Set, reset, clear the fingerprint scan
- Output for all the different LED status lights
- Input from the door contact
- Lock/unlock output
- Output door state to chamber sensing controller

Table 14 below, shows a comparison of the microcontrollers we have considered. It can be noted that the cost of each chip has not been taken into account as they are all relatively cheap making the cost insignificant when making the decision on which to use.

Table 14 - Security Microcontroller Comparisons

	MSP430 G2553	**MSP430F G4618**	**MSP4324 01R**	**MSP4324 01M**	**ATMEG A328**	**ATtin y25**	**ATtiny 417**
CPU	MSP430	MSP430	ARM Cortex - M4F	ARM Cortex - M4F	AVR	AVR	AVR
Frequency (MHz)	16	8	48	48	20	20	20
Non-volatile Memory (KB)	16	116	256	128	32	2	4
RAM (B)	512	8k	64k	32k	2k	128	256
GPIO Pins (#)	25	80	84	84	23	6	6
I2C	1	1	4	4	1	1	1
SPI	2	1	8	8	2	1	1
UART	1	1	4	4	1	0	1
DMA	0	3	8	8	0	0	0
Analog Digital Converter	ADC10	ADC12	ADC14	ADC14	ADC10	ADC 10	ADC10
ADC Channels	8	12	24	24	8	4	4
Comparators (Inputs)	8	8	8	8	1	1	1
Timers - 8-bit	0	0	0	0	2	2	1
Timers - 16-bit	2	2	4	4	1	0	2
Timers - 32-bit	0	0	2	2	0	0	0
Boot Strap Loader	UART	UART	UART/I2C/ SPI	UART/I2C/ SPI	UART/I2 C/SPI	I2C/S PI	UART/I 2C/SPI
Min VCC	1.8	1.8	1.8	1.8	1.8	1.8	1.8
Max VCC	3.6	3.6	3.6	3.6	5.5	5.5	5.5
Active Power (uA/MHz)	330	400	400	400	200	200	200
Standby Power (uA)	0.7	1.3	1.3	1.3	0.75	0.75	0.75
Wakeup Time (us)	1.5	13	13	13	60	60	60

From the options listed in Table 14 below, shows a comparison of the microcontrollers we have considered. It can be noted that the cost of each chip has not been taken into account as they are all relatively cheap making the cost insignificant when making the decision on which to use.

Table 14 - Security Microcontroller Comparisons the ATMega328 microcontroller is our best option. Compared to the other Atmel options and the options we researched from Texas Instruments, the ATMega328 has the lowest power

requirement as well as one of the lowest standby current draws, has enough GPIO pins as well as analog channels, and covers all of the voltages of the different sensors it will be connected to. It also has the ability to communicate over UART which will be used for transmitting data to the main communication controller.

3.5 Isolation and Damping

One of the more difficult obstacles within our project comes from isolation and damping required to give our sensors reliable accuracy within our chambers. This problem is partially due to the noisy neighbor problem as well as any unexpected loud external noise or vibrations that could generate false positives within our chambers. We will explain the noisy neighbor problem and go over some possible solutions and determine which solution or combination of solutions would best suit our needs.

3.5.1 The Noisy Neighbor Problem

In communications, there is a similar problem to what we have to deal with called the Exposed Node Problem. The exposed node problem in communications is when transmission nodes in a network are within range of each other and they begin to interfere with each other. The interference happens when a node tries to send a message out, and another uninvolved node wrongly thinks that it will cause collision if it transmits its own message. This problem overall slows transmission rates of networks and may cause backups.

The reason this situation is important to us is that we have a similar problem to solve in regards to the individual observation chambers of the device. We are calling it the Nosy Neighbor Problem. We need to isolate each individual observation chamber of the device from the sensory influences of the other chambers. Without proper isolation of the observation chambers, one chamber may have its sensory threshold reached by a phone going off in another chamber, leading to false positives for the sensors in the observation chamber and causing unnecessary alert transmissions and possible race conditions, overall leading to a system slowdown. The sensors for the device measure vibrations, which is the periodic oscillation of particles in an elastic body. For the purposes of this product, we will look at mechanical vibrations and sound as two different topics, even though vibration and sound studies are closely associated with each other. In our product, we have both acoustic vibration (sound) and mechanical transmission vibration, so we need to reduce the effects of the vibration actuators between chambers via some form of Acoustic Quieting.

3.5.2 Acoustic Quieting: Isolation vs damping

When managing vibrations in mechanical and electromechanical systems, there are two common approaches; Vibration Isolation, and vibration damping. The damping of a vibration involves the removal of energy from a vibration wave entering a system. This is normally accomplished by layering materials of varying density to deal with resonant frequencies in the entering wave and reduce the energy in the transmission wave. The isolation of a vibration involves the deflecting of specific frequencies in the attempt to prevent the vibration from entering the system. This is done through steel springs, rubber or other elastomeric pads, or isolation bellows. Many vibration isolation systems have some type of damping in them as systems with little or no internal damping will have uncontrolled resonant motion at certain frequencies that will be transmitted to the support structure. This resonant motion may degrade the support structure and eventually cause it to fall apart. Because of the nature of our system, we will look into isolating vibrations caused by the phones vibrator motor and damping ringing of the phone between the individual chambers.

3.5.3 Damping Sound

The speaker of the phone is not in contact with the system the same way the phone and its built in vibration motor will be. The speaker on the phone will propagate a sound vibration in all directions, and that sound will bleed through the walls of the observation chamber and any openings in the chamber. This leads to a nosy neighbor problem in which the neighboring observation chambers may listen in on the actuating phone in the source chamber. We need to prevent the sensors in the other observation chambers from hearing the phone in the first chamber as much as possible. We also need to prevent the sensors from hearing the outside as much as possible. The figure below illustrates what needs to be accomplished.

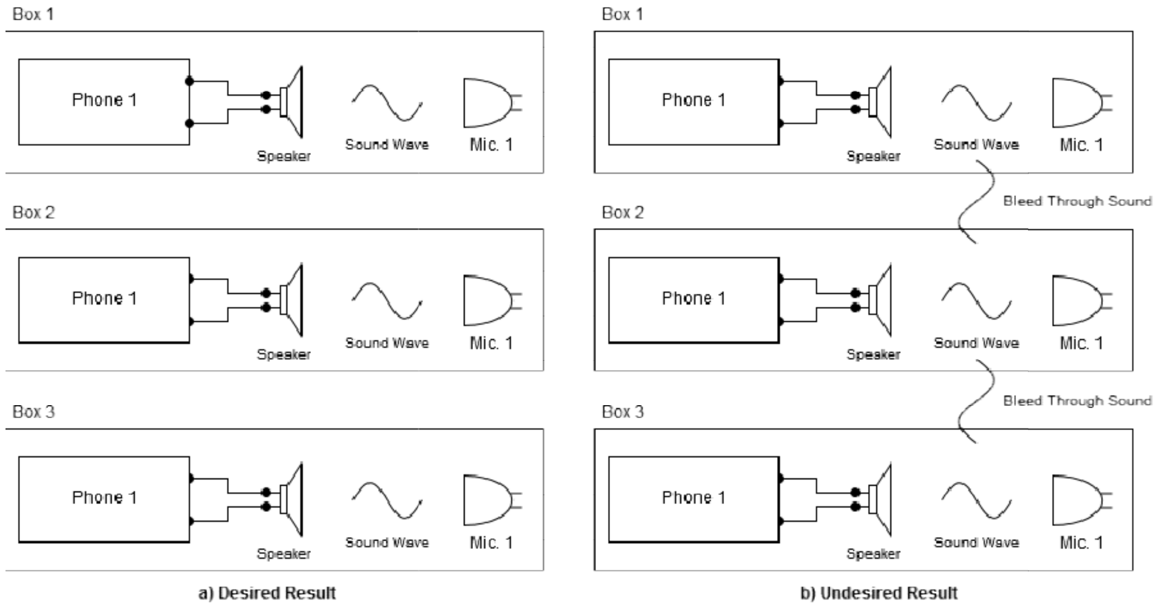


Figure 35 - Desired vs undesired vibration sensing

There are a few ways for us to damp the sound between the walls of the device such as with sound absorbing foam, structural damping, and mass loaded vinyl.

3.5.3.1 Sound absorbing Foam

Acoustic soundproof foam prevents sound waves from reflecting off of hard surfaces like ceilings and walls. Instead of allowing sound waves to reflect, soundproofing foam absorbs sound waves, resulting in quiet environments with little echo. The material does not completely block out noise, just dampens it. Acoustic foams are capable of damping and absorbing sounds across multiple frequencies, minimize reverberation, and overall help prevent sound from bleeding through walls if installed properly. Acoustic foam in often used to control noise for machine rooms, equipment enclosures, computer rooms, and manufacturing facilities. The ability of a soundproofing foam is usually represented with a Noise Reduction Coefficient (NRC) value falling between 0 and 1, with a value of 0 denoting perfect reflection of sound and a value of 1 denoting perfect absorption of sound. [20] However, many distributers and marketing engineers know how to manipulate the test data and skew results unfairly at times. Testing methods for acoustic absorbers are defined by the American Society for Testing and Materials (ASTM), which requires all members to follow the same rules. However, a flaw in the testing method does not take into account the edges of acoustic absorbers. During testing, the edges of an acoustic absorbing material are exposed, however, the calculation for the absorption coefficient only takes into account the front surface and ignores the edges entirely. This leads to inflation in NRC values that can lead to some NRC values being greater than unity, which is illogical. In actuality, it’s not illogical to think that the actual NRC values of a material are 66%-86% of what the manufacturer has published. The better value to look for is test results in sabins, which is an absolute measure of absorption independent of surface area that allows two absorbing materials to be directly compared on equal terms. However, many manufacturers do not publish their test results in sabins. Below is a table of a few soundproofing foam products we are considering for the product.

Table 15 - Soundproofing Considerations

Material	**125 Hz**	**250 Hz**	**500 Hz**	**1000 Hz**	**2000 Hz**	**4000 Hz**	**Overall**
Foam Factory: 1” Wedge	0.14	0.17	0.36	0.47	0.51	0.61	0.4
Foam Factory: 2” Wedge	0.2	0.29	0.66	0.8	0.89	1.02	0.65
Foam Factory: 3” Wedge	0.25	0.47	0.83	0.82	0.92	1.04	0.75
Foam Factory: 4” Wedge	0.39	0.61	0.91	0.79	0.95	1.03	0.8
Convoluted Acoustic Foam Panel 1”	0.13	0.23	0.5	0.82	0.96	0.94	0.65
Acoustic Foam Panel 1”	0.19	0.32	0.85	0.88	0.58	0.5	0.65
Acoustic Foam Panel 2”	0.32	0.75	1.2	1.1	0.9	0.63	1
Acoustic Foam Panel 3”	0.49	1.03	1.27	1.18	1.03	0.72	1.15

The above table shows the absorption properties of a few different foam products at different thicknesses given in NRC values. What we see first is that the thicker the material is, the more porous, or absorptive, the material is as the NRC value approaches a value of 1. We also notice that Foam Factory wedge foams have higher NRC values in the higher frequencies than the acoustic foam panels and the convoluted acoustic foam. Acoustic Foam panels do better in the low frequencies than the Foam Factory wedge foams, making them better bass absorbers. We can also look into Eggcrate foams. Foam Factory has 1.5” Eggcrate rated at 0.45 NRC overall and 2.5” Eggcrate rated at 0.6 NRC overall. We know that the NRC values are skewed to a degree, however, this will likely be the route we go for damping the sound in the observation chambers. Soundproofing foam is cheap and quick to install. If we combine the soundproofing foam with some other building materials, we can acquire a good transmission loss at a relatively cheap price. During installation, we can use acoustic adhesives such as Green Glue to further enhance soundproofing. Because Green Glue can be applied with a simple calking gun, it makes overall installation easier, less time consuming, and ultimately cheaper.

3.5.3.2 Structural Damping

One way to dampen sound in systems is to build the structure of the system with materials that have good transmission loss characteristics. Materials such as low density metal and wood tend to have poor transmission loss characteristics, while glass, dense metal, brick and mortar have relatively good transmission loss characteristics. These common construction materials may not necessarily provide as good of a sound barrier as other engineered materials, but certain arrangements of these materials may provide similar and maybe even better sound blocking than engineered materials. The table below shows a couple of common building materials and their transmission loss characteristics.

Table 16- transmission loss characteristics

Material	Thickness [mm]	125 Hz	250 Hz	500 Hz	1000 Hz	2000 Hz	4000 Hz
Plywood	6	17	15	20	24	28	27
Plywood	18	24	22	27	28	25	27
Laminated Glass	13	31	38	40	47	52	57
Hollow Cinder Block (unpainted)	100	22	27	32	32	40	41
Hollow Cinder Block (painted)	100	22	30	34	40	50	50
16g Galvanized Sheet Steel	1.6	14	21	27	32	37	43
3mm Lead Sheet	3	28	32	33	32	32	33
Hardwood (Mahogany)	50	19	23	25	30	37	42
1.5 mm lead between two sheets 5mm plywood	11.5	26	30	34	38	42	44

What the table above shows is that the transmission loss characteristic depends on the material, the thickness of the material, and the arrangement of different materials. Dense materials such as the cinder block, hardwood, laminated glass and lead sheet have high transmission losses in the higher frequencies, meaning that are effective at blocking higher pitch noises. However, the hardwood, and the plywood as well show relatively low transmission losses in the lower frequencies, meaning they are bad at blocking low frequency bass noises. Certain adhesives such as cement base paint and green glue can also improve the transmission loss of the material. Adding cement base paint to the cinderblock did little for improving the rejection of bass frequencies, but adds almost 10dB to transmission loss in higher frequencies. We can see that combining a lead sheet with two 5mm plywood sheets improved the transmission loss characteristic across the entire frequency sweep, with the lead sheet improving the weak bass frequency loss of plywood by almost 10dB and the two sheets of plywood adding loss to the high frequency loss of the lead sheet. The combination of materials made the constructed sheet better in rejecting bass frequencies and higher frequencies than the hollow unpainted cinderblock as well as the mahogany at a fraction of the space. We include the laminated glass to show that certain materials are very effective at blocking sounds at many frequencies. We will likely not use laminated glass for this product due to how expensive and difficult it would be to work with it. We will likely use an assembly of cheap materials such as drywall and plywood with air gaps in order to create effective transmission loss at low cost and at the sacrifice of some space.

3.5.3.3 Mass Loaded Vinyl

Mass Loaded Vinyl (MLV) is a limp mass material made of high temperature vinyl used for the purpose of reducing the magnitude of airborne sound transmission through walls. The material has a rough weight of 1 pound per square foot, making it roughly as dense as lead. Due to the high density, Mass Loaded Vinyl makes for a good sound blocker, rather than a sound absorber. Mass loaded Vinyl is also very thin, coming pretty standard at either 0.125” or 0.25” in thickness, meaning it can improve the sound transmission loss of a barrier while taking up little space. Unlike most other high mass sound blockers such as drywall, gypsum boards, concrete, hardboard, and concrete masonry units, Mass Loaded Vinyl is also very flexible, meaning that it can accommodate and be molded for many different shapes[21]. On top of its ability to be molded, it works better as a sound blocker than stiff high mass materials because it is limp and partially gives way when sound waves hit it. Most Mass Loaded Vinyl products are rated at 1-lb/ft^2 and 2-lb/ft^2. The more dense that the material is, the better transmission loss characteristic it has. Mass Loaded Vinyl is commonly used for blocking sound transmission between building walls, floors, ceilings, and as acoustic wrap. For our purposes, we would be wrapping individual observation chambers of the device to block the sound of phones from entering other chambers. The table below shows a few Mass Loaded Vinyl products we were looking at, showing their transmission loss characteristics across a range of frequencies.

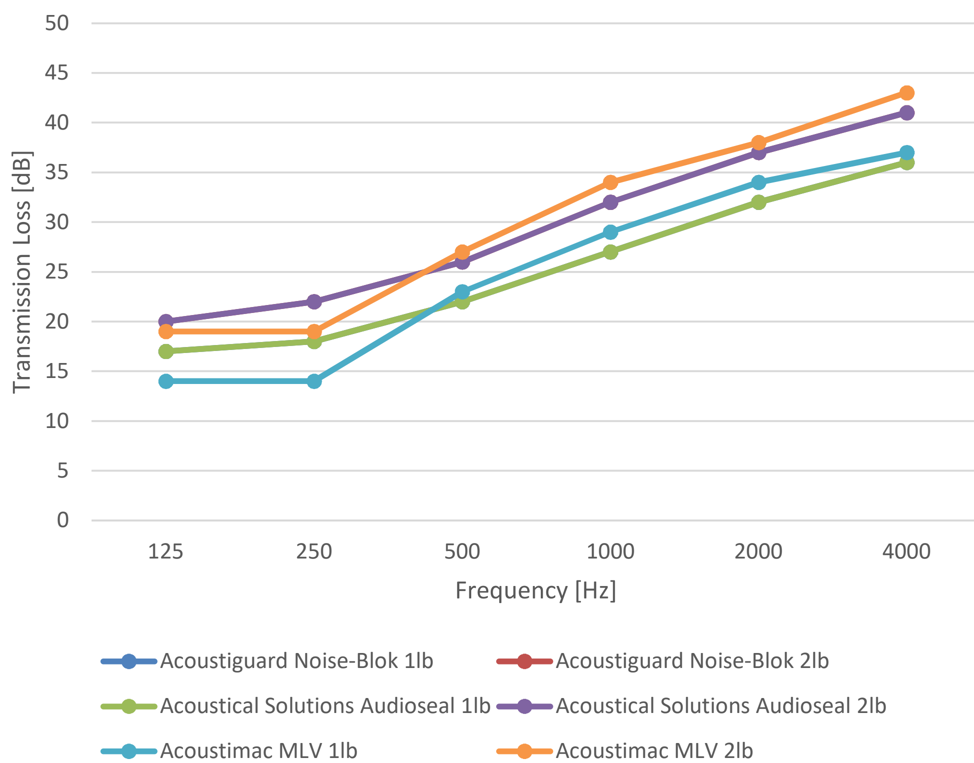


Figure 36Transmission Loss of various MLV Products

Noise-Blok and Audioseal have perfectly identical transmission loss characteristics that improve gradually as frequency increases (which is why you can't see any characteristic curves both the 1-lb and 2-lb rated Noise-Blok products). Acoustimac MLV has poor transmission loss in low frequencies (125-500 Hz), but has better transmission loss characteristics in the higher frequencies. Mass loaded Vinyl falls in to a sound transmission class in the early thirties, which is very high for such a thin material. Because of the good transmission loss characteristics of the material, we wouldn't need many layers, meaning we don't have to use as much material. The main drawback of this material is that it is expansive. One roll of 1-lb rated Mass Loaded Vinyl can easily cost over $100. The other methods of blocking sound may prove to be better for our budget.

3.5.4 Damping and Isolating Mechanical Vibration

Mechanical vibrations are involved in any and all systems that contain either moving parts, or is subject to outside forces. There are two major types of vibrations in mechanical systems. Free vibrations, and forced vibrations. Free vibrations are momentary disturbances to systems that are allowed to move unrestrained under said disturbances. In practice, these free vibrations normally will eventually damp back down to equilibrium. The type we really care about for this product are forced vibrations. Forced Vibrations happen when energy is added to a system in which the vibration is driven by an external agency. These forced vibrations are usually periodic and can be harmonic or non-harmonic. Particularly interesting are the systems that undergo simple harmonic motion with sinusoidal forcing. Such as our system where the forced vibrations are induced by a small vibration motor inside of a phone. Improper management of these harmonic vibrations leads to resonance, which is caused when the driving frequency approaches the natural frequency of free motion. This leads to an increase in the magnitude of the vibration, which allows more energy to be transferred across the entire system as vibrational force. For the product we are building, this is a very bad thing as resonant vibrations or any vibrations carried through the structure of the system can cause interference with our sensors designed to sense mechanical vibration. If the vibration motor in a phone of one observation chamber causes resonance, the vibration sensors in another observation chamber may be able to observe those vibrations, and then we have another Nosy Neighbor issue, causing false positives. We need to get around this problem. The diagram below illustrates how this Nosy Neighbor problem shows up with mechanical vibrations and how we want the system to be observed.

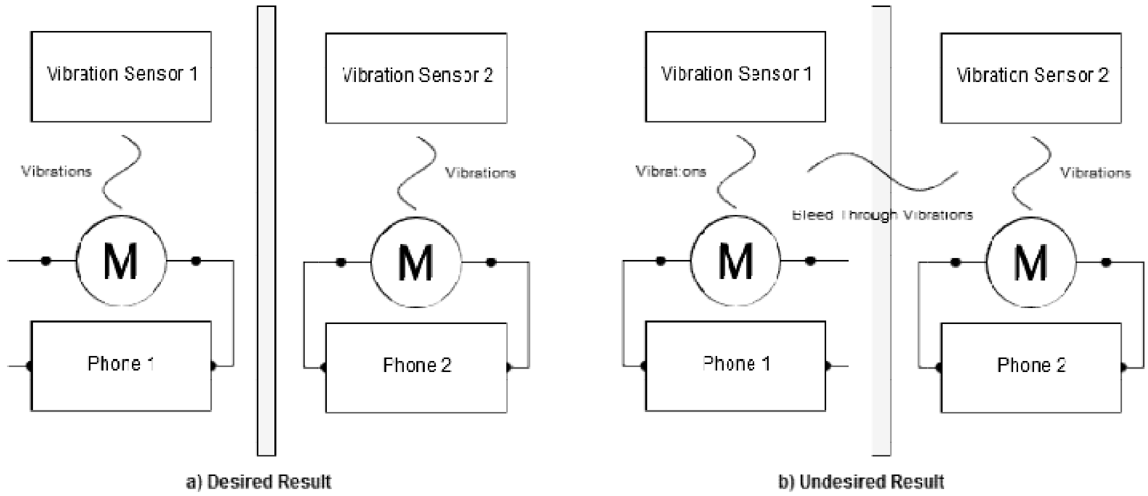


Figure 37 - Desired vs undesired vibration sensing

One method of dealing with this is to damp the mechanical vibrations. Mechanical damping is the attenuation of the vibratory movement of the system, or the removal of energy from the system. Depending on the way the vibration is induced, damping can be accomplished with the implementation of dry-friction interfaces, viscous damping, mechanical spring systems, and the integration of elastomeric engineered materials.

Because we are not dealing with parts that move a ton, we don’t need to use a dry-friction interface. The moving parts we are dealing with also are not very heavy, so a spring system is not practical for our purposes either. Viscous damping and other elastomeric materials will suit our purposes quite well.
Elastomeric materials and the materials used for viscous damping are called viscoelastic materials. Viscoelastic materials exhibit properties of both liquids (viscous materials) and solids (or any elastic materials), which have very useful material behaviors under impulse shock and periodic shock. Viscoelastic materials are capable of removing energy from vibrations by absorbing them and releasing energy as low level heat, or by changing the frequency of the vibration to one that will not resonate with other components of a machine.

Via the use of viscoelastic materials, we will be able to achieve three types of damping: unconstrained, constrained, and tuned damping.

3.5.4.1 Unconstrained Damping

In unconstrained damping, a viscoelastic pad is made for a machines moving parts, and that pad is placed between the parts causing excess vibration and the rest of the machine. As the machines parts move, the viscoelastic pad conforms its shape in order to absorb some of that energy and release it out of the material as low level heat. This removes some vibration from the system and prevents machines from breaking down. Because there is little finite control implements in this type of damping, it is the easiest method to address vibrations in a system.

This will likely be the damping method this product will implement as we do not need extremely finite vibration control.

3.5.4.2 Constrained Damping

Similar to unconstrained damping, this damping method involves a viscoelastic material conforming to the movement of a machine in order to absorb energy. In constrained damping, however, the viscoelastic pad is lined with a flexible metal plate to add efficiency to the damping. This method is used in order to gain more finite control of vibrations.

3.5.4.3 Tuned Viscoelastic Damping

Tuned damping, or directed damping, is for when we need to keep specific wavelengths out of the system. This damping methods main purpose is to get resonant frequencies out of the system before they cause serious damage. Because we don't have parts that can be easily damaged by vibrations, we do not need this much control in the system.

3.5.4.4 Isolation and Damping

Vibration isolators and vibration dampers are often confused because many common vibration isolators also display some inherent damping. A vibration damper takes mechanical energy out of the system. While a proper spring system or rubber mounts may make good isolators, they have little damping properties. Vibration isolators will lower the natural frequency of a system to a frequency below the frequency of excitation. This helps prevent the transmission of vibrations throughout the system, but does not inherently weaken them. The diagram below shows what a vibration damper and isolator look like in concept.

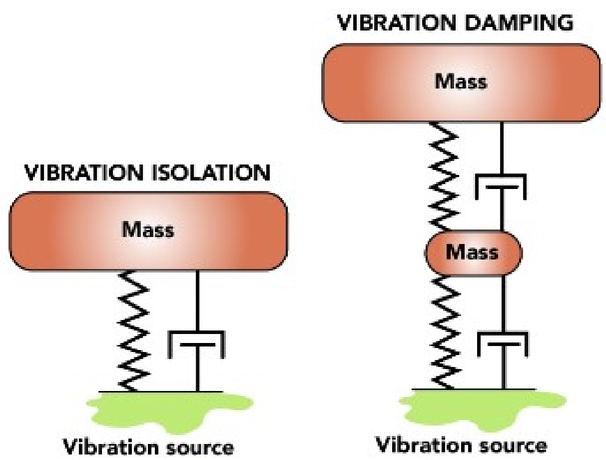


Figure 38 - Vibration Isolator vs Vibration Damper

For the purposes of this product, we will be looking primarily at solutions for isolating vibrations. The vibration motors in phones are not likely to damage any of the components in the product. What we are concerned about is reducing the transmission of vibrations across the entirety of the system in order to prevent sensors from observing vibrations they should not be observing. However, many vibration isolators also exhibit some damping properties, which hinders their life a little bit, so that will be something to take into account.

3.5.5 Viscoelastic Materials as Vibration Isolators

Viscoelastic materials are designed to distribute force in all directions when under stress and strain, similar to a fluid, and then return to their original form when no longer under stress, similar to a solid. These properties make viscoelastic materials ideal at controlling vibrations in systems. For our product, we are looking at a few viscoelastic materials in order to control vibrations from phones: natural rubber, urethane, neoprene, and sorbothane.

3.5.5.1 Natural Rubber

Polyisoprene, or natural rubber (NR) as it is often referred to as.

3.5.5.2 Urethane

Urethane is a man-made rubber designed to outlast natural rubber in a number of ways. Compared to natural rubber, urethane is much more resilient to adverse environments, meaning it will not easily degrade when exposed to greases, oils, oxygen, ozone, sunlight, and high temperatures. Urethane can also be very hard with durometer ratings in the 90's at the cost of some compromised physical properties. Polyurethane is designed to retain its physical properties at high stiffness. Urethane is abrasion resistant, and has good load bearing. Urethane does not easily deform which is good. Urethane also, very interestingly, is semi-conductive and can assist in minimizing the severity of electrostatic discharge. On top of all this, because urethane is used in the manufacture of many different products, we can get urethane in different forms such as solids and foams. Below is a chart showing some of the urethane products we are considering.

Table 17 - Urethane Properties

Product	Durometer	Rated Load (lbs)	Diameter (in)	Height (in)
AAC V10Z60-MF1U0424	24	0.3	0.28	0.32
AAC V10Z60-MF2U0624	24	0.6	0.405	0.5
AAC V10Z60-MF2U0824	24	0.6	0.405	0.5
ESP 9.9528	Soft 70A	N/A	0.28125	0.5
ESP 9.9529	Firm 95A	N/A	1.9375	0.65652
ESP 9.9530	Medium 88A	N/A	1.5	0.75

The nice thing about urethane dampers for us is that we can get them for small rated loads, which is great considering how light phones are today. The main holdup for us right now is that some of these urethane dampers are rather expensive for us. Some of these are almost 12 dollars each. Another thing about urethane is that they have a very limited effective operation temperature range.

The AAC urethane dampers are at peak performance only at a range of 32 to 90 degrees Fahrenheit. For our purposes, this should be fine since ideally, our product will be indoors and will be at room temperature (70 to 75 degrees Fahrenheit). However, if the product is used in environments exposed to higher than room temperature heat, then we may see a decrease in performance. We can look further into this material for our vibration damping and isolation as it does show promise.

3.5.5.3 Neoprene

Neoprene is a viscoelastic material that is designed to have very high resiliency when exposed to many different chemicals and high temperatures. Unlike natural rubber, neoprene will not easily break down when exposed to heat, oil, ozone, and other general chemicals. The material will also retain its integrity in temperatures approaching 200 degrees Fahrenheit, making it ideal for environments with machines that give off a lot of heat. Neoprene is also fire resistant, which makes it further useful in high temperature environments. Neoprene is also available in a range of hardness grades and thicknesses, making it commercially versatile. Another advantage of neoprene is that is has low damping, but it makes an excellent vibration isolator. Neoprene is often used for anti-vibration pads, steel acoustic isolators, acoustic structural bearings, and isolators for machinery and plant equipment. Below is a table showing off a few neoprene products we are considering.

Table 18 - Neoprene Considerations

Product	**Duro**	**Rated Load (lbs)**	**Deflection (in)**
Kinetics RDA-55	50	55	0.4
NPS-2-45	N/A	100-240	0.05
Acoustical Surfaces ND-A	30	45	0.35
Newport NP-20A	N/A	25	N/A
Isotech NCM1Y	35	45-75	0.35

Unfortunately, though neoprene is relatively cheap and extremely durable, it is also very stiff. That stiffness makes neoprene, as it is commonly manufactured, to be rated for weights that are much higher than we need. A typical phone only weighs 0.22 – 0.44 pounds. Currently, the Newport NP-20A is the best one we found, but implementing that would require us to add a large amount of weight to make the supported load high enough to achieve proper vibration isolation.

3.5.5.4 Sorbothane

Sorbothane is a polyether based polyurethane engineered for improved viscoelastic properties. Sorbothane is effective along a range of temperatures going as low as -29 degrees to 71 degrees Celsius. Sorbothane is also a highly damped material, making it very good for applications which operate near resonant frequencies. The physical properties of Sorbothane allows Sorbothane to damp vibrations by turning mechanical energy into heat via molecular friction. Due to how highly damped the material is, Sorbothane controls shock (Figure 39) and vibrations (Figure 40) quite well. Figure 39 shows the shock response of Sorbothane compared to some other damping materials. In the figure, we can see that Sorbothane reduces the impact force of the impulse almost 80% and slowly brings the response to rest. The slow deceleration is overall accommodating to devices and prevents them from being damaged. We can also see that Sorbothane has little ringing and a very low rebound compared to some other viscoelastic materials.

Figure 40 shows the vibration response of Sorbothane, and we can see that Sorbothane has a considerably lower transmissibility at resonance compared to other viscoelastic materials. The low transmissibility will mean that vibrations from the phone are less likely to be carried through the system because there is little amplification of those vibrations. This is what we want in regards to isolating the vibrations from the phone.

The nice thing about Sorbothane is that it comes in many different shapes and weight ratings for many different applications. They come with different finishes to handle weather or heated environments. Some come with and adhesive included. The really beneficial thing about Sorbothane though is that it is really cheap. We can get four hemisphere pads of Sorbothane for around seven dollars, which is perfect for our application.

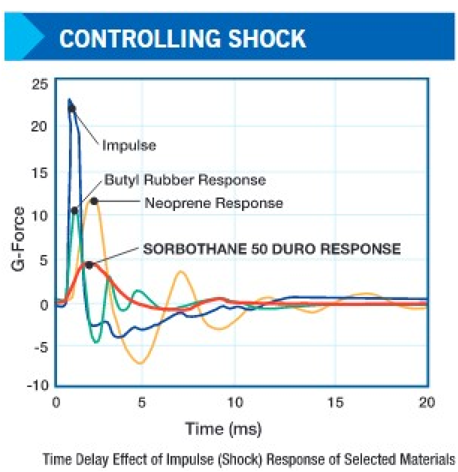


Figure 39 - Sorbothane Shock Response

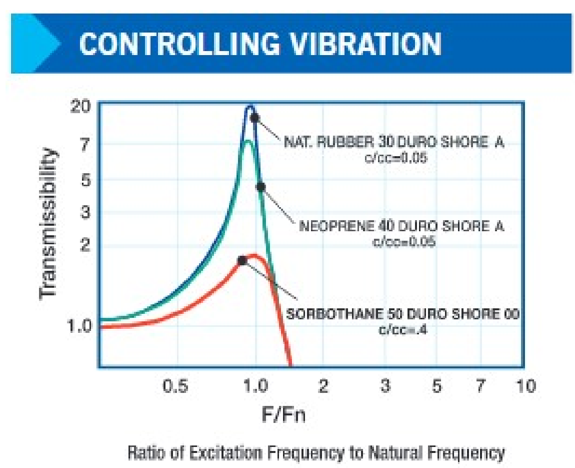


Figure 40 - Sorbothane Vibration Response

The shape we will look at primarily for our product is the hemisphere pad. We choose the hemisphere over other Sorbothane shapes because they are cheaper, but more importantly, they have the lowest weight rating. Sorbothane needs a 20% compression to get the best isolation from the pad. Most phones these days only weigh 100-200 grams (0.22-0.44 pounds), and the smallest hemispheres (0.5”x0.25”) are rated for 0.2-0.5 pounds. Depending on the arrangement of the pads, we may have to use a weighted plate to assist the compression factor of the pads. Below in Table 19, we are showing the data of the Sorbothane pads we are considering.

Table 19 - Sorbothane Pad Comparisons

Product	Part Number	Diameter	Height	Duro	Rated Load (lbs)
Hemisphere	0510100-30-10	0.50	0.25	30	0.2 - 0.5
Hemisphere	0510100-50-10	0.50	0.25	50	0.3 - 0.7
Hemisphere with PSA	0510101-30-10	0.50	0.25	30	0.2 - 0.5
Hemisphere with PSA	0510101-50-10	0.50	0.25	50	0.3 - 0.7
Hemisphere with PSA & Urethane Coating	0510104-30-10	0.50	0.25	30	0.2 - 0.5
Hemisphere with PSA & Urethane Coating	0510104-50-10	0.50	0.25	50	0.3 - 0.7

PSA is an aggressive pressure sensitive adhesive meant to very securely bond the pads to another surface, useful as it reduces error in shape factors due to trying to manually apply adhesive. The thin urethane coating reduces some surface friction, while also protecting the pad from the elements. The loss of friction is not very appealing for us. Because we are not yet sure of the arrangement of the pads, we are also looking at the higher Duro versions of each pad type in the event that we need to use a weighted plate to accommodate the arrangement of the pads. Our current most appealing Sorbothane pad for the product is the Hemisphere with PSA

4.0 Project Design

In this chapter we will cover all of our design decisions that have been made and the reasoning behind them. We will include the considerations that were taken into account for each decision as well as why believe our decision is the best option for our project.

4.1 Hardware Design

This section is going describe the hardware components of our design and how they all fit together and work together to achieve our design goals. It will cover the requirements of the individual parts and explain each part is needed.

4.1.1 The Power Circuit

The power circuit is the heart of the hardware design. Without getting power properly distributed, nothing else will work correctly. Below in Figure 41, we have a layout of how our power will be distributed evenly throughout our design as a whole.

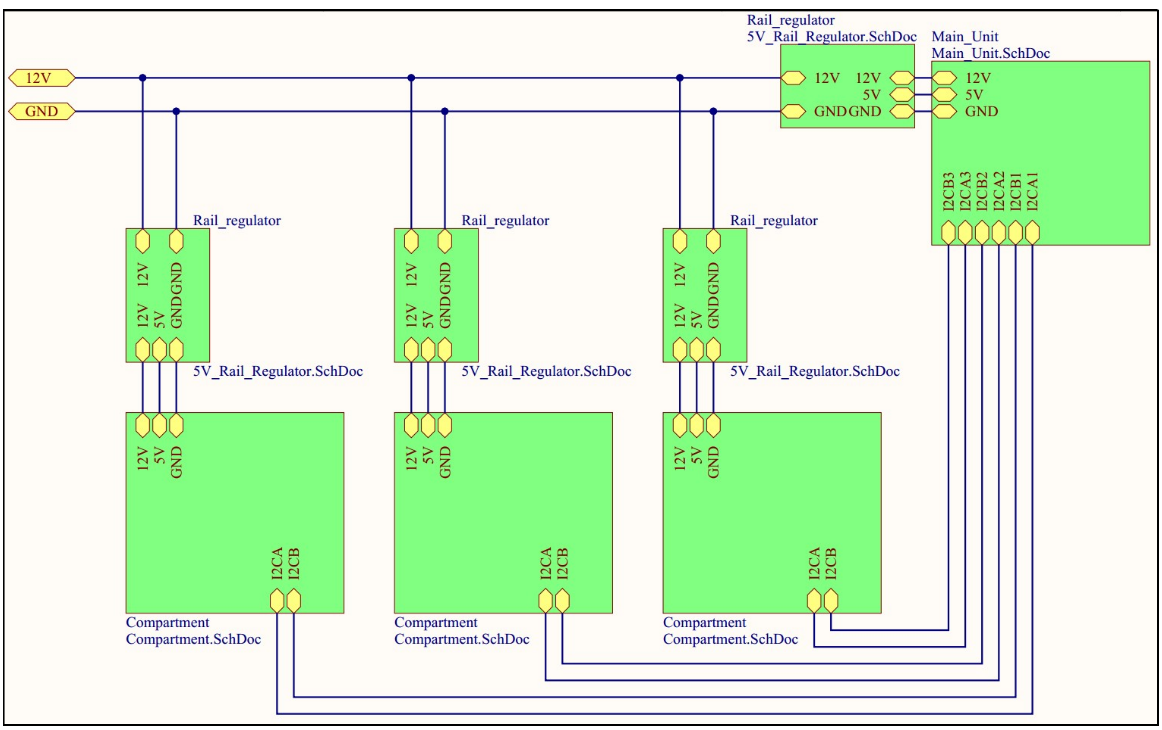


Figure 41 - Top Level Power Distribution

Within our top level power distribution, you can see the three compartments and the main communication unit (the Beaglebone) which are all fed with the same 12 volt unregulated power supply. Each compartment and the main controller will have a 5 volt rail regulator module that is shown in Figure 42.

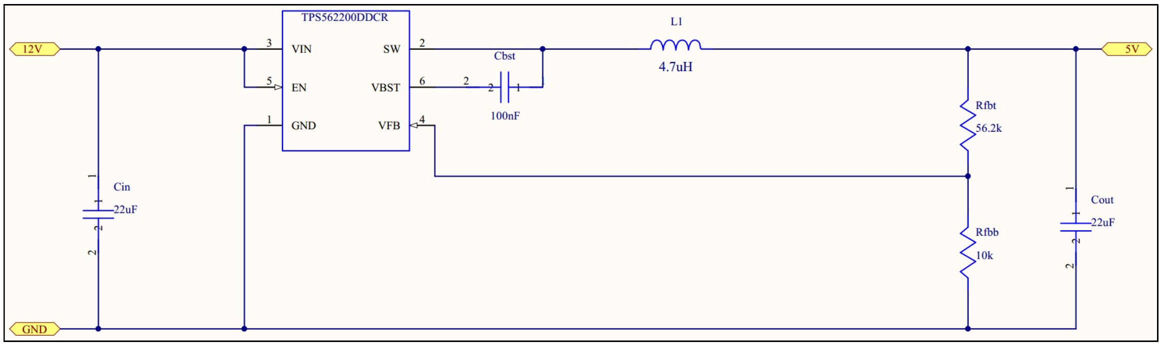


Figure 42 - 5 Volt Regulator from 12 Volt source

4.1.2 Modularity consideration

The system, ideally, will be modular to allow for growth. Since there are a large amount of parts that require relative consistency among the voltage inputs, the design has to keep smooth voltages in mind. There will likely be smoothing capacitors at the input to the circuit, to prevent a large voltage spike when the compartment gets connected. With modularity in mind, the schematic for the individual compartments will be identical within each compartment as shown in the compartment schematic below in Figure 43. Within the schematic there are two subsystems; the sensor subsystem and the locking subsystem.

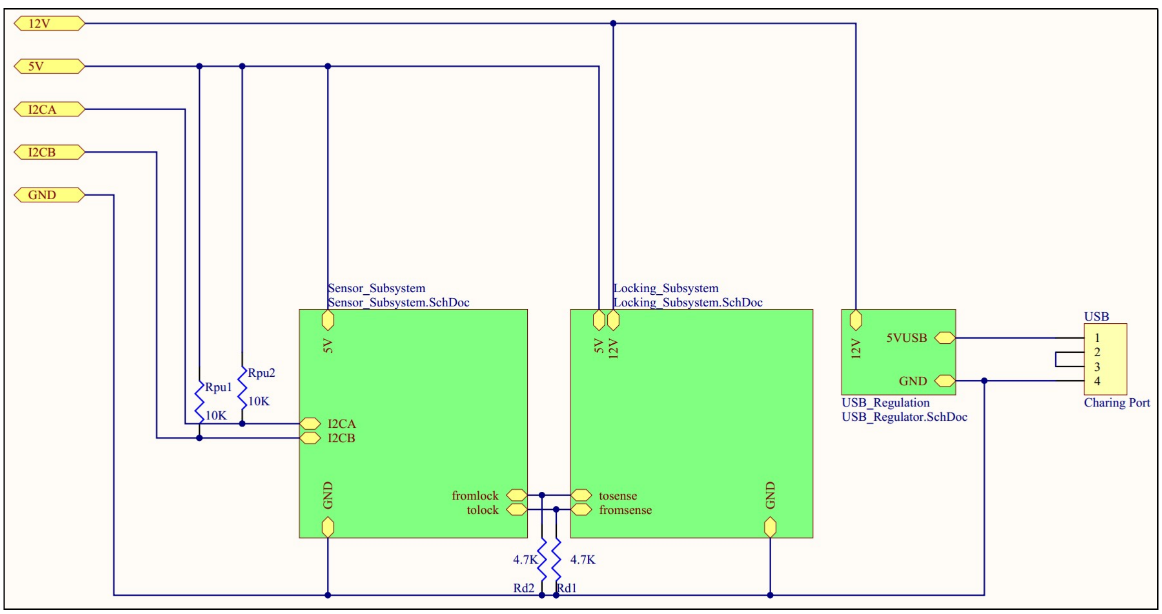


Figure 43 - Compartment Schematic

4.1.3 Separating Security and Sensor Microcontrollers

In our design the box uses two different microcontrollers (Not including the one that is onboard with the fingerprint scanner) with discrete jobs. Primarily the reasoning is that the regular atmega328p would not have enough GPIOs (General Purpose Input/Output pins), but there are a few reasons we chose this as the solution, rather than simply choosing another MCU or using a pin multiplexer. A list of additional problems that contribute to the solution are as follows.

4.1.3.1 Collision Prevention

The first additional consideration that this would address is collision prevention. The relationship between the fingerprint scanner and whatever microcontroller it is hooked up to is a master-slave relationship. In order for this relationship to be a fluid and intuitive one, the fingerprint scanner would need to be the master, as it is the device that gets notified when the finger is pressed to the scanner. If that microcontroller were also the sensor data collecting and interpreting microcontroller then it would also be a slave to the Main_Unit, and this will cause for a problematic issue. The microcontroller being a slave to two devices will ultimately cause collisions, even in the most rigid and discrete state machine. This would have to be handled with software, wasting clock cycles, and causing a greater amount of complexity to the code, which would then lead to a much larger response time on interrupts. While this time may seem negligible on paper, in practice it causes a large deal of problems in the timing of detectors, sensors, and accuracy. With a dual microcontroller setup, pipelining can be implemented very effectively, and allow multiple parallel tasks to run on at the same time. (e.g. an information request about the sensor data from the Main_Unit will not interrupt a person scanning their fingerprint, and cause the lock to open for too short of a period of time, or a mismatch in data verification.)

4.1.3.2 Priority and response-time

A common mistake when setting up a microcontroller to do many different tasks simultaneously is the lack of priority considerations, and the actual feedback time on interrupts for large complicated body loops. It is not an infrequent occurrence for two kinds of interrupts having similar priority, and a choice to be made arbitrarily. In our design, the locking and unlocking of the box definitely comes first, but for the interpretation and sensing of the data to be accurate, the sensing needs to be as continuous as possible. False flags for a failed unlock attempt (e.g. someone else trying to unlock the wrong box) would could easily cause a disturbance in the read. From an ITsec consideration, this would be a huge opening for a DOS(Denial of Service), or Brute force exploit.

4.1.3.3 Failsafes

In any electronic locking mechanism, the power outage condition will always be a possibility, and will need to be considered. Having two separate microcontrollers allows us the opportunity to add a backup power circuit (likely a battery backup) to only the locking mechanism. In the event of a power failure, it isn’t a high priority to maintain all the systems in a notification reporter when the power goes out, but it’s very likely that it would be of high priority to be able to retrieve your cellphone. There will likely also be another physical variation of this consideration, but for it to still be a secure option, it would need to have the extra added hassle of a backup key. With this alternative, it would allow for an alternative failsafe that does not require an official to come by and open the box, which would streamline any kind of power outage response tremendously in the situations where it might apply.

4.1.3.4 Wrap-up

Ultimately having two separate microcontrollers for these two tasks, allows the two tasks to be entirely discrete, and give us the opportunity to prevent any sort of biometric data leakage back to the Main_Unit, as the two controllers can be connected by one or two digital pins for a status or specific request. This discretization reduces system complexity, secures the system, and allows for failsafes, where using a different microcontroller or adding a pin expander would simply be an oversight response, rather than a functional design consideration.

4.1.4 Sensors Subsystem

The vibration sensor is actually a passive component, that produces voltage, so this will not need to be powered, but rather, isolated to prevent it from becoming a vibration plate (instead of a vibration sensor). The vibration sensor will be a rather trivial issue, but the microphone circuits will not be. This will be touched upon further in the sensors section, but the microphone circuits will involve a decent amount of floating voltage comparators, which means it's not simply relying on a common ground for reference. The voltages will need to be regulated, and not have any slew rate inconsistencies between the two. No matter the kind of regulation used for the whole circuit, or the running voltage of the circuits themselves, these will be on their own linear voltage regulation to prevent that sort of issue. This is a heavy redundancy, and likely unnecessary, but it is important that the two microphones have similar outputs by the time they reach the differential comparator. The sensor subsystem controlled by an ATmega328 is shown below in Figure 44 and it has two subsystems of its own.

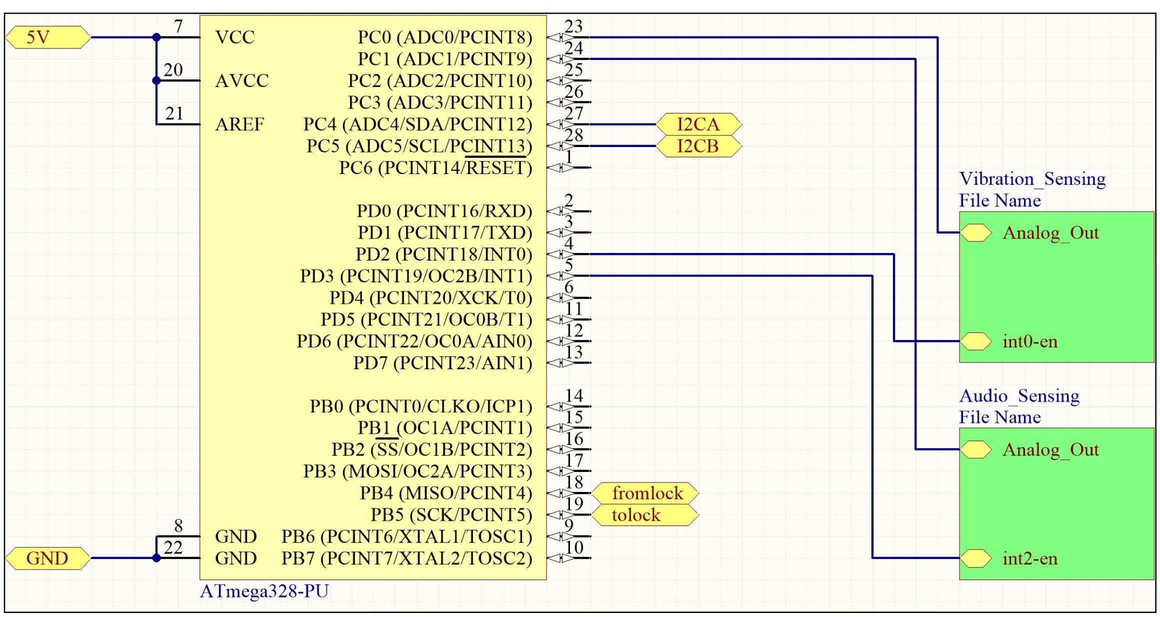


Figure 44 - Sensor Subsystem

4.1.4.1 Vibration Subsystem

The vibration subsystem that makes up part of the sensor subsystem is shown below in Figure 45. It converts the vibrations from the phone into a voltage that is then amplified to a point where it can be easily distinguished by the microcontroller.

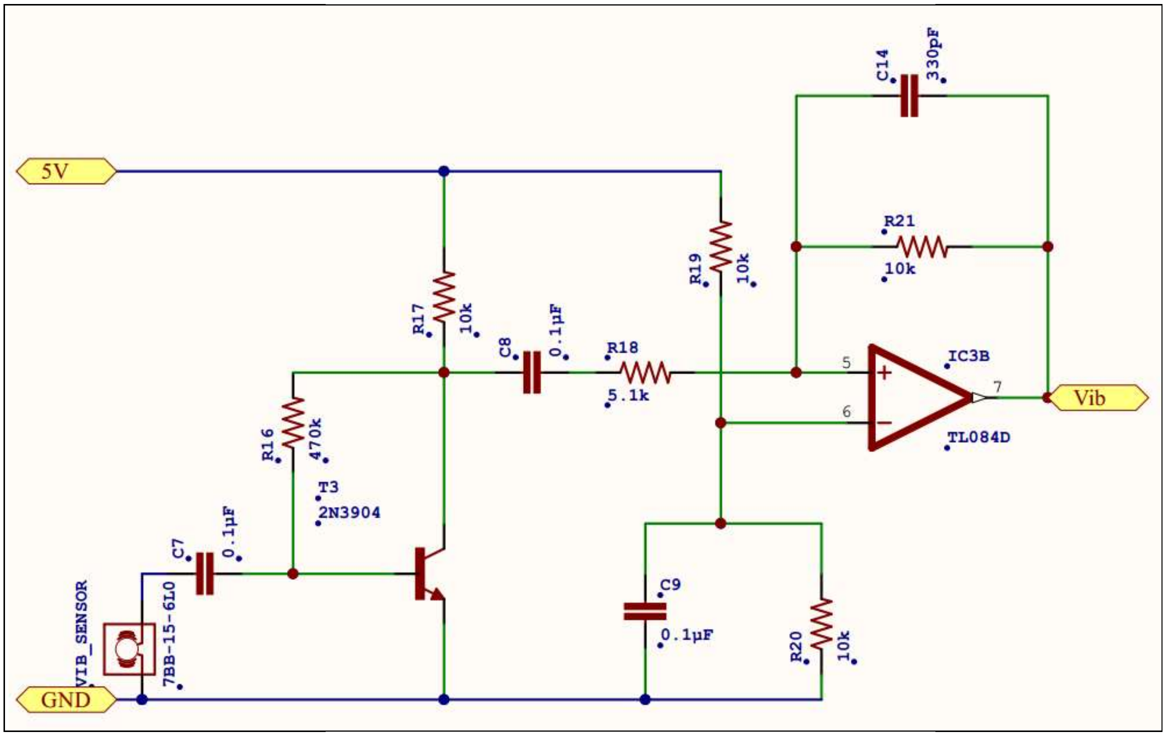


Figure 45 - Vibration Subsystem

4.1.4.2 Audio Sensing Subsystem

The microphone subsystem is a bit more complicated than the vibration sub system. It is designed to take it a separate signal from 2 different microphones. And amplify them an equal amount. Then the processed signals get sent to the microcontroller where comparisons will be made and appropriate actions will be taken.

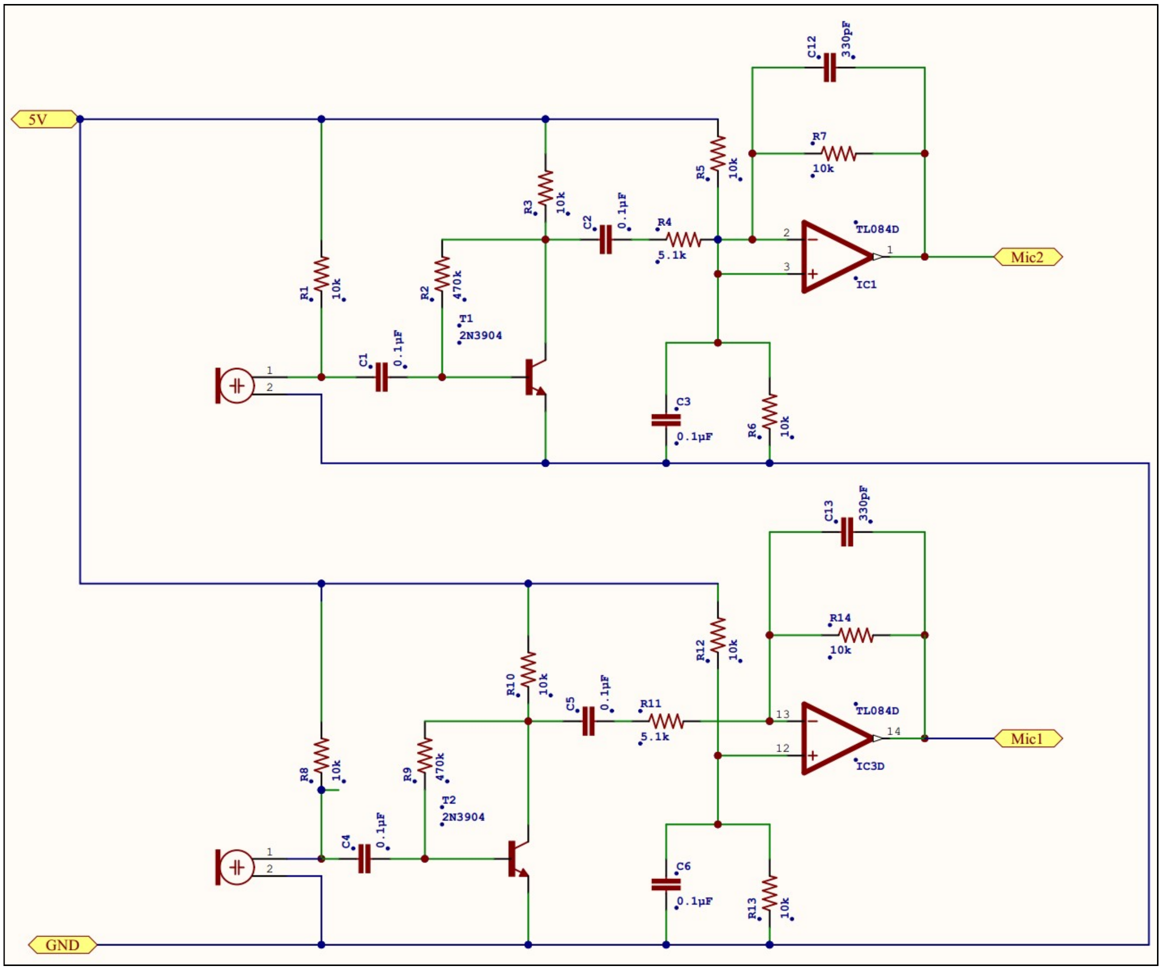


Figure 46 - Audio Sensing Subsystem

4.1.5 Security Subsystem

Within the locking subsystem that is referenced in the compartment schematic shown in Figure 43, we have the solenoid lock as well as the fingerprint scanner. The overall security subsystem is show in Figure 47.

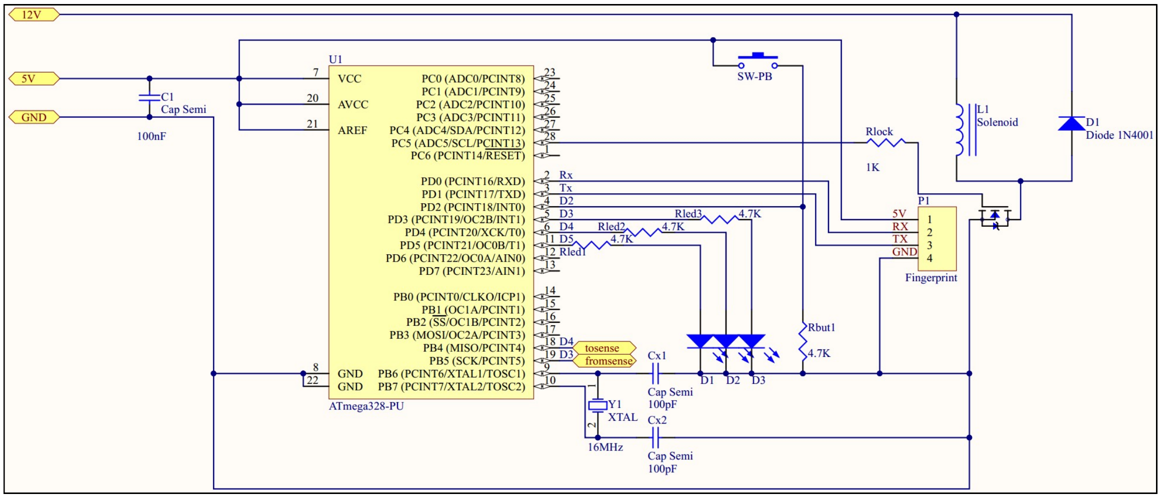


Figure 47 - Security Locking Subsystem

4.1.5.1 Solenoid Lock

The current solenoid being tested will require a 12V at 300mA output for a short period of time. This will ideally use a relay and a smoothing capacitor. Given 4 of them and the +20% rule, we will need a peak output power of about 35W + regular operating power. This is well within our operating conditions of 200W In order to operate these it will be best to use Solid state relays or a similarly functioning power driving circuit using a properly biased power FET.

4.1.5.2 Fingerprint Scanner

The fingerprint scanner we will be using will have a nominal working voltage of about 5V for power, but a UART interface voltage of 3.3V, which means it will be likely that our microcontroller will need to be a 3.3v or we will need a bidirectional level converter for the UART channel to communicate properly. [2] [3] Regardless, it will be important to include a 3.3V regulator into the circuit. Whatever decision we use for the microcontroller regulation (switching or linear) will be chosen for this one.

The logic level converter will require a 3.3V regulator as well. Since we will be likely coming from 5V to a high impedance input pin, a fixed output, positive linear regulator will suffice.

Table 20 - 3.3V fixed output linear regulators comparison

Part	Price($)
L78L33ABZ-AP [25]	0.41
LD1117V33 [26]	0.56
L78L33ACZ [27]	0.35

We will be going with either the LD1117V33, which, depending on vendor, has a rated current of about 0.8A and an average price of 0.56 due to timing and availability, or the L78L33ACZ, which has a 100mA rating and is 38% cheaper, due it not being a high current output. Our most probable candidate for implementation is shown below in Figure 48.

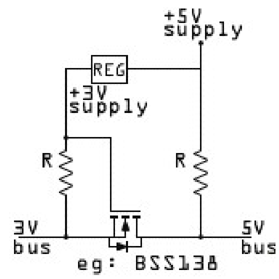


Figure 48 - Example circuit of the level shifter

4.1.5.2.1 Compatibility Considerations

Differing GPIO logic levels bring up a possible concern. In the circuit design, there are a couple components that will have to be connected together which do not share the same logic level. The Atmega328 has a operating logic voltage of 5v, while the Beaglebone has a logic level voltage of 3.3V. [15] The Fingerprint sensor also has a communication logic level voltage of 3.3V. This means we will need a level shifter. We could choose between an already implemented design, like the Sparkfun Logic Level Converter - Bi-Directional, or a resistor voltage divider, or a circuit using a low voltage based FET.

4.1.5.3 USB-Related

USB power standards, for charging, has a requirement of 5V along the power rails, and a limit to the current of 2.5A. It’s pretty common practice to limit this to at most 2.4A. For ease of testing and limitations, we will limit the current to around 1.5-2.0A this will also limit the max power consumption and not have to worry as much about energy loss due to heat. For the sake of keeping heat on the chip to a minimum and independent consistency across all USB ports, we will be using separate voltage regulators for each USB charging port.

Table 21 - choices for USB power regulators

Regulator	**Vin**	**Vout**	**Iout (cont)**	**Cost**
LTM8062[5]	3.3-15V	3.3-15V	2.0A	10-15$ per
LM3525[4]	2.7-5.5V	N/A	0.5-1.5A	1-2$
LTC3601	4-15V	0.6-14.52V	1.5A	3-4$
LT8606	3V-42V	5V	350mA	3$
LT8608[6]	3V-42V	5V	1.5	$3

To reduce circuit complexity, we will likely be using a switching regulator such as the LT8608, as it is the least expensive can achieve our desired output.

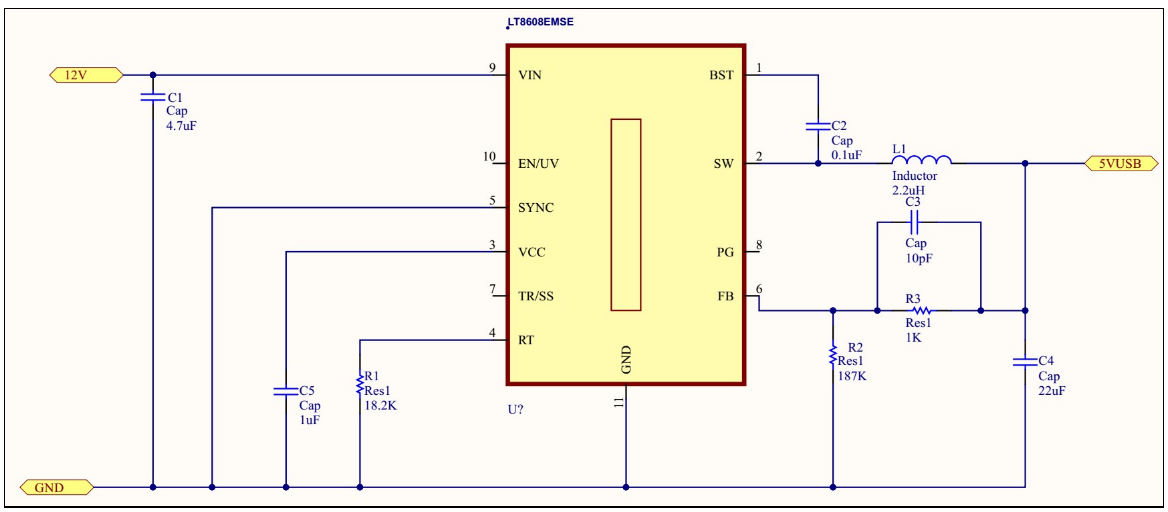


Figure 49 - USB Regulator

4.1.5.4 Contact Rails

To ensure the most simplicity in the design, while offsetting as much of the circuitry off the boxes as possible, the compartment rail contacts will contain a common ground, an unregulated 12V contact and a regulated 5V rail. Depending on the power consumption of the box, we will choose between a switching and linear regulator. Ideally, this will be a linear regulator for simplicity, however, a switching regulator will no longer be reasonable if the 5V rail will consume greater than 1A.

Table 22 - Comparison of 5V regulator choices for the 5V rails

Linear Regulator	**Vin(V)**	**Vout(V)**	**Iout(A)**	**Cost($)**
LT3080-1[7]	4.8 - 28	0-Vin	1.1	2.69
LT1085[8]	>=6.5	5	3,5,7.5	4.75
LT3083 [10]	1.2-23	0-Vin	3A	6
LTM8001[12] *(5V regulator)*	Jun-36	1.2-24	1.1A parallel	25-60
Switching Regulator				
LTM8064[11]	7.5-58	1.2-36	7A max	23
LTM4634 [13] (3V regulator)	4.75-28	0.8-5.5 0.8-13.5	5,4	51
LTM8073[14]	3.4-60	0.8-15	3 (cont) 5 (peak)	15.11

4.1.5.5 Microcontroller related

Since it is highly likely that the microcontrollers will be using a small amount of current, we will be using linear regulators for them. While there are regulators on board for most microcontrollers, it would be ideal to keep that off chip to minimize the heat dissipation, and improve the efficiency of the controller.

Table 23 - Table of regulators for the Microcontrollers ideally ones that can do 3.3 or 5v

Linear Regulator	Vin	Vout (V)	Iout(A)	Cost*($)
LT1764A[9]	2.7-20	Fixed: 1.5, 1.8, 2.5, 3.3 Adjustable: 1.21-20	3	$4.71
LT3080-1[7]	4.8 - 28	0-Vin	1.1	2.69
LT3083 [10]	1.2-23	0-Vin	3A	6.00

Table 24 - All-in-One Solutions

Device	Unit Price ($)	Amount Required per Channel	Total Cost per channel ($)	Bidirectional?
Sparkfun Logic Level Converter - Bi-Directional [16]	2.95	1/4	0.74	y
SparkFun Level Translator Breakout [17]	6.95	1	6.95	y
SparkFun Voltage-Level Translator Breakout - TCB0104 [18]	3.95	4	0.99	y
LTC1555LEGN-1.8 [19]	4.65	1	4.65	y
LTC1555LEGN	2.14	1	2.14	y
TXB0104QPWRQ1	1.42	4	0.35	y

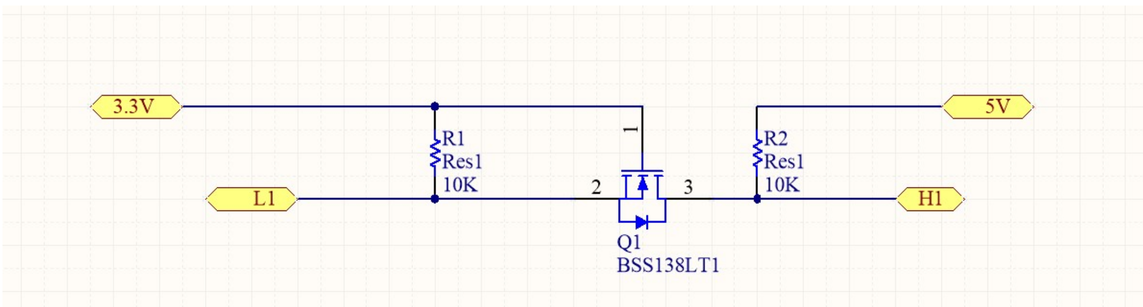


Figure 50 - Example logic level shifter with low vgs-th mosfet

The choice seems to be a toss up between a TXB0104QPWR and a BSS138L. To reduce on cost, space, and heat, we will be going with the BSS138L with either a single mosfet design, or a complete CMOS design.

Table 25 - Mosfet Drain Current Comparison

Mosfet	Drain Current(mA)	Price($)
BSS138L/BVSS138L[20]	200	0.063
DMC2400UV-7 [21]	570	0.41
ALD212900PAL[22]	79	0.29
ZVN2110A[23]	320	0.36
ZVP2110A[24]	-230	0.53

4.1.5.5.1 Solenoid Powering

Because the Arduino does not have a 12V 0.6A output, we will need to find a way to switch the 12V-Unregulated on and off the solenoid latch. We have the option to choose a mosfet driving circuit, an SSR, a regular Relay, or a BJT. A regular relay would cost too much and be overkill. An SSR would likely be a similar, but less extreme case. This leaves a BJT and FET circuits.

4.1.6 Ethernet For Communication

Using ethernet from the Main_Unit to communicate the notifications within the restricted area was ultimately decided for a number of reasons, including design simplicity, Implementation Simplicity, expansion, and ultimately cost.

4.1.6.1 Implementation Simplicity

The first acknowledgement that need to be taken when making this decision was the likelihood of an infrastructure already existing. Coax isn't as common or abundant as ethernet, as it is mainly used for TVs and specialized equipment. While this would likely fall under the specialized equipment category, if such a solution hasn't already been made, it is most likely due to the initial investment that would need to be made. Requiring a technician to come in and install different instruments throughout the restricted area would require a lot of an initial time, setup, and cost investment. The same consideration applies to fiber optics, but to a greater extent. Fiber optics are usually reserved for a need-based application. Shielded, twisted pair (The standard in Cat5e [1]) is plenty, and for most applications fiber optic cable would be excessive at best. Using ethernet for the implementation allows the compartments to be reduced to an Internet of Things(IoT) consideration, rather than a large infrastructure installation.

4.1.6.2 Design Simplicity Consideration

Using ethernet allows for the design to be simple. Cat5e, and TCP/UDP networking protocols are longstanding industry standards, which means that there are already existing components for every Main_Unit we have considered. This reduces on the complexity in the hardware design and in the programming.

4.1.6.3 Expansion

As has been stated plenty of times previously, it has been a standard for a long time, so there are plenty of black box solutions for both cat5 to fiber optic conversion and cat5 to coaxial cable conversions for less than $100, which allows for it to expand over different mediums. Since it will be a hosted application, this allows for the administrators of said device to allow for digital signage, intercom notifications, tuning for when a notification is worth being made, integration into existing computers, and even offsite monitoring if one would so choose. Mixed with the right internal component communication topology, it could be easy to implement overrides from a privileged user account on the beaglebone.

4.1.6.4 Cost

Using cat5e would allow for a minimized up-front cost. Allowing the compartments to be managed by cat5e allows for any adopter to save a lot of money on having to install any parts than necessary. Even if an infrastructure would be needed to implemented, it is still cheaper to implement a cat5e network than it would be to implement a fiberoptic or coaxial network, by the price-per-foot alone. This also allows for the reduced cost of components because the Main_Unit already has an ethernet port built in and implemented.

4.2 Proposed System Software Design

This section will cover the proposed system software design. As shown below in Figure 11, we have a system flow diagram showing the major functions of the currently proposed system.

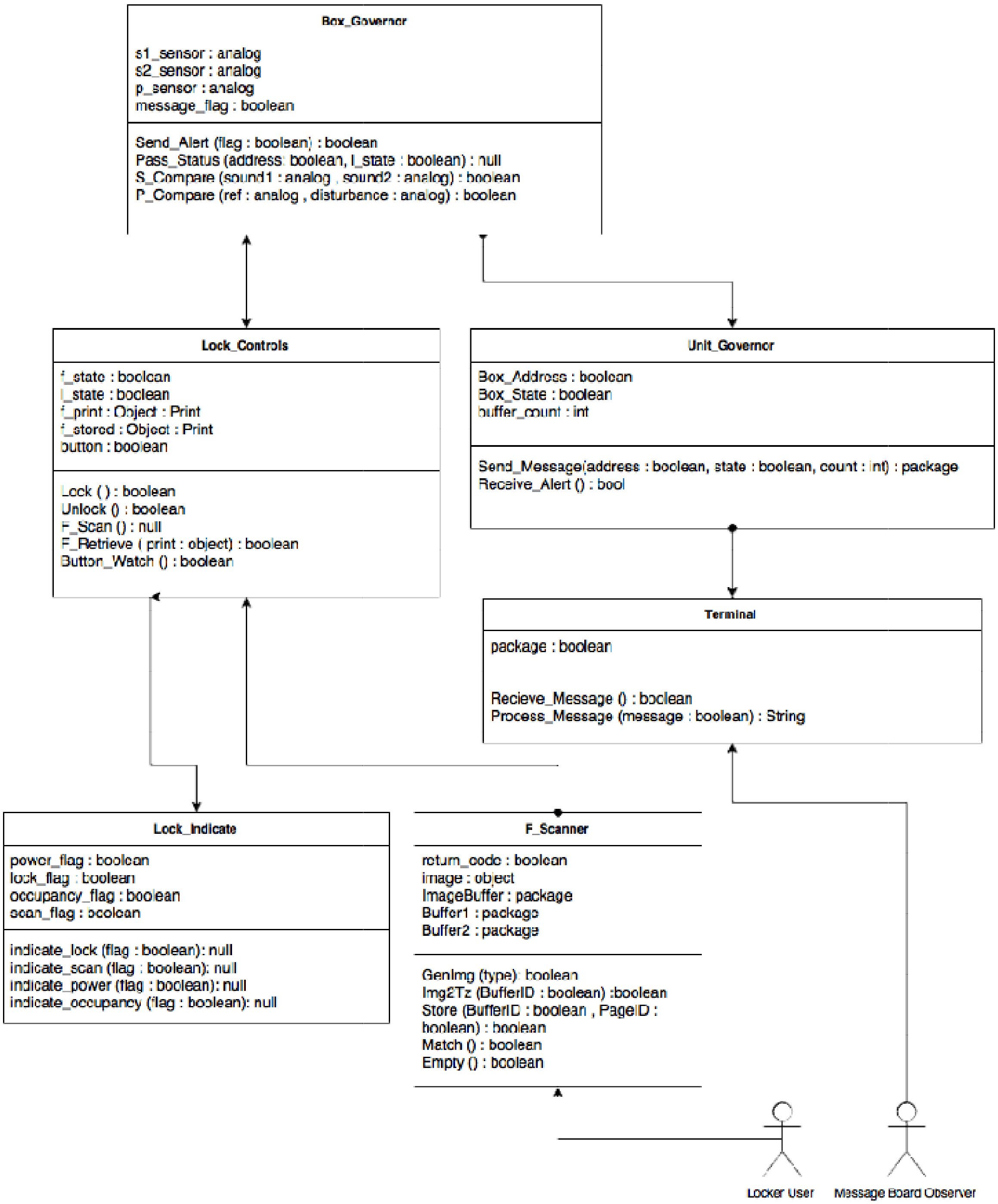


Figure 51 – Process Flowchart

The diagram is split into a few different functional blocks that cover a specific area of functionality of the device. The diagram shows the individual variables and methods used in each functional block, as well as the direction of data flow and even which points in the system the user interacts with the system. This section will cover the different functional blocks and components inside of them.

4.2.1 Terminal

The user terminal is the main point of access for the user that is watching over the indication messages the unit governor sends. This is the computer where a lobby person monitoring the phones or the phone owners will be able to see the messages that the device sends out when the device detects a phone ringing or vibrating. Most of the functions and variables in this block deal with receiving a message package sent by the unit governor and then translating that to a message into a form to be printed on screen. The following are the variables and functions for the terminal:

- **Package:** This variable is the last message the terminal received from the unit governor. The message received by the unit governor should contain an address of origin, and a type code. The type code will denote either common contact, or emergency contact depending on certain conditions.

- **Receive_Message():** This method is a small method that facilitates the receiving of a message sent to the terminal from the unit governor. This method will verify successful receiving of package and send out a response code. After verifying successful transmission, this method will then call the method Process_Message().

- **Process_Message(package):** This method will take in the data stored in variable package and process what type of message to send. This method will look for an address and type code and then print out the appropriate message to the terminal.

4.2.2 Unit Governor

The unit governor watches over all of the box governors in the system. This unit keeps a list of all of the box governor addresses, the state of the box they are reporting, as well as keep a running list of the number of consecutive messages the unit governor receives from the same address. This unit also passes messages to the terminal to the terminal for processing. Only one of these units will exist in each full device. The following is a list of variables and methods for the unit governor:

- **Box_Address**: This variable will store the addresses of all of the box governors being monitored in the system. This variable is important for facilitating the generation of package headers for transmission.

- **Box_State**: This variable is a two bit flag that will facilitate the generation of a package header that tells whether or not the box governor is active, and whether or not it has received an update.

- **Buffer_Count**: This variable is a running count of the number of consecutive times the unit governor has received an alert from the same address. This variable is important to help facilitate the generation of package headers during transmission.

- **Send_Message(address, state, count):** This method will take in the date from the address variable, the state, variable, and the count variable, and then use that data to generate a transmission package. Once the package is made, this method will send the data to the terminal unit.

- **Receive_Alert():** This method will be called when the unit governor receives an alert from the box governor. This method will look at the address of the message origin, pull the state and update the running count for consecutive alerts. After storing that data, this method will call Send_Message() to send an alert to the terminal.

4.2.3 Box Governor

This unit is important and has many functions. This unit watches over all of the sensors in each individual box and passes information to the unit governor when the sensors are triggered. This unit will process any inputs from the sensors to make sure the input does not read as a false positive for a detected disturbance. This unit will also send information to the indicator unit for displaying certain diagnostics. One of these units can be found underneath each individual observation chamber. The following is a list of variables and methods for the box governor:

- **S1_Sensor:** The first audio detector in the box. This variable stores an analog level of volume that the first microphone detects. This information is used in the method S_Compare() for determining validity of the internal sound disturbance.

- **S2_Sensor:** The second audio detector in the box. This variable stores an analog level of volume that the second microphone detects. This information is used in the method S_Compare() for determining validity of the internal disturbance.

- **P_Sensor:** The piezoelectric sensor that is used to measure pressure and vibration in the box. This variable stores an analog level of pressure exerted on the sensor. This data is used in the method P_Compare() for determining validity of the internal vibratory disturbance.

- **Message_Flag:** This variable is a single bit flag denoting that the box governor has confirmed positive for an internal disturbance. This is used to determine when to call method Send_Alert().

4.2.3.1

- **Send_Alert(address, flag):** This method will send an alert to the unit governor in the event of a positive trigger for an internal disturbance. This method will take in the flag input and send out a package with the address of the box governor to the unit governor.

- **Pass_Status(P):** This method is used for passing a diagnostic bit to the indicator unit. If the piezoelectric vibration sensor has any type of consistent output on it, this method will send a flag to the indicator unit to show that there is something occupying the box.

- **S_Compare(S1, S2):** This method is used to help assist in reducing the nosy neighbor problem in this device. If the sound sensors pick up a disturbance, this method will take the input of the two sound sensors, compare them with each other, and if the results are similar, the method will set a flag and call the Send_Alert() method.

- **P_Compare(reference, P):** This method is used to verify that a disturbance has hit the piezoelectric vibration sensor. This method will compare the values of the disturbance with a reference value, and if a certain threshold is met, this method will set a flag denoting positive for an internal disturbance and call the method Send_Alert().

4.2.4 Lock Controls

This unit is the primary security implement of the device. This unit handles the authentication of the fingerprint scanner, print retrieval, the actuation of the locking mechanism, as well as handle the code to start the locking procedure. This unit will also send data for security diagnostics to the indication unit. Without this unit, there would be no security for the user to safely place their cellular device into this device. There will one of these attached to the box governor in each individual observation chamber. The following is a list of variables and methods for the lock controls:

- **f_state:** This variable is a single bit flag telling the lock control unit the current status of the fingerprint scanner. If the flag is true, it means that the fingerprint scanner is currently primed to scan for a print. If this flag is false, then the fingerprint scanner is not primed to scan for a print. This information is used to determine the course of action of the indicator unit.

- **l_state:** This variable is a single bit flag telling the lock control unit the current status of the locking mechanism. This flag will be true for actuated and false for released. This information is used the help determine the course of action the F_Retrieve() function as well as determining the course of action the indicator unit.

- **f_print:** This variable is a buffer variable for the print currently being scanned. If the variable f_stored is equal to null, then this variable will be copied into f_stored. The print stored in this variable is compared to the print in f_stored when verifying if the scanned print is a match for the purpose of unlocking the observation chamber.

- **f_stored:** This variable will store the image of the fingerprint that will be used to verify if the user scanning their print is the correct user. This variable will be compared to f_print during the verification process.

- **button:** This variable is a single bit flag representing whether or not a button is engaged. If this flag reads false, it means the button is currently idle. If this flag is true, it means that the button is currently being pressed. When this flag becomes true, the Button_Watch interrupt will be called.

- **Lock():** This method will handle the locking procedure for the observation chamber. When this method is called, the controller will send a signal to actuate the locking mechanism. At the same time, this method will also update the locked status indicator to true and send a flag to the indicator unit to update the shown status of the lock.

- **Unlock():** This method will handle the unlocking procedure for the observation chamber. When this method is called, the controller will send a signal to release the locking mechanism. At the same time, this method will also update the locked status indicator to true and send a flag to the indicator unit to update the shown status of the lock. This method will also call Empty() to wipe the stored print data from memory.

- **F_Scan():** This helper method will call any of the methods needed to scan the fingerprint of the user. This method will facilitate the generation of a fingerprint image, the formatting of the data, and then the storage of that data to a specified address in memory.

- **F_Retrieve(print):** This method will deal with verifying the input and exit operations for the overall authentication procedure as shown in the decision tree in Figure 52. This method will call F_Scan(), and then verify what is currently in memory. If this method calls F_Scan() and there is no fingerprint in memory, this method will run code to add a print into memory and then call Lock() to secure the device. If this method calls F_Scan() and there is a print in memory, this method will start calling the Match() method of the fingerprint scanner to verify that the print being scanned is a match with the one in memory. If the print doesn't match, the method will be terminated. If the prints match, this method will then call the method Unlock() to release the lock on the device. The chart below shows a representation of this decision process.

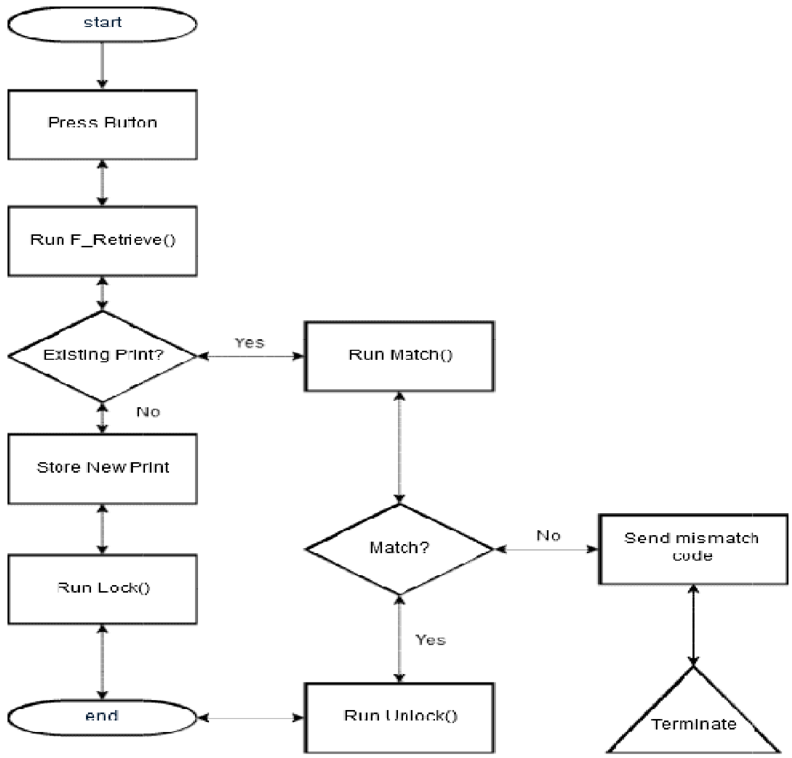


Figure 52 - F-Retrieve() Decision Tree

Button_Watch(): This method is an interrupt that will trigger when the user presses the button next to the fingerprint scanner. When this method is called, the device will start to call the methods associated with scanning a fingerprint and verifying whether the print on the scanner matches the print stored in memory.

4.2.5 Lock Indicate

This unit handles all of the scripts associated to controlling indicators. The indicators will be LED lights to represent certain diagnostics such at the status of the lock, whether or not the device has power, whether or not the fingerprint scanner is engaged, and as well as showing whether or not the box is currently occupied. This unit will receive all of its diagnostic information from the box governor and the lock controller. The following is a list of variables and methods for the lock indicate:

- **power_flag:** This variable is a single bit flag indicating the current status of the power circuit. This flag will be true if there is currently power running through the system, otherwise this flag will be false when there is no power. This information will be used to determine the action of the power indicator.

- **lock_flag:** This variable is a single bit flag indicating the current status of the locking mechanism. This flag will be true if the locking mechanism is currently engaged, or if the lock has been closed, otherwise this flag will be false when the locking mechanism is not engaged, or the lock is open. This information will be used to determine the action of the lock indicator.

- **occupancy_flag:** This variable is a single bit flag indicating the current status of the piezoelectric sensor. This flag will be true if there is currently a voltage across the terminals of the piezoelectric sensor denoting that there is a mass on the sensor. If there is no consistent voltage across the terminals of the sensor, this flag will read false. This information will come from the box governor and will be used to determine the action of the occupancy indicator.

- **scan_flag:** This variable is a single bit flag indicating the current status of the fingerprint scanner. This flag will be true if the fingerprint scanner is currently primed and scanning for a fingerprint, otherwise this flag will be false when the scanner is no longer seeking a fingerprint. This information will be used to determine the action of the scanner indicator.

- **Indicate_Lock(l_flag):** This method will run a script to turn the locked indicator light on or off. If this method is passed a false flag (the lock is unlatched), the light will turn off. If this method is passed a true flag (the lock is latched), the light will turn on. This functions main purpose is to tell the user when the box is locked.

- **Indicate_Scan(s_flag):** This method will run a script to turn the scan indicator light on or off. If this method is passed a false flag (the fingerprint scanner is not currently primed to scan for a fingerprint), the light will turn off. If this method is passed a true flag (the fingerprint scanner is currently primed to scan for a fingerprint), the light will turn on. This functions main purpose is to tell the user when to place their finger on the fingerprint scanner to have an image generated.

- **Indicate_Power(p_flag):** This method will run a script to turn the power indicator light on. This indicator light will essentially be on at all times provided the device is running. If this method is passed a false flag (there is not enough power from the outlet), the light will turn off. If this method is passed a true flag (the device is on and operational), then the light will be turned on. This function will serve as a visual que showing when the device is actually plugged in and operational.

- **Indicate_Occupancy(o_flag):** This method will run a script to turn the occupied indicator light on. If this method is passed a false flag (meaning the piezoelectric sensor has nothing on it and there is no voltage across the sensor), then the indicator light will turn off. If this method is passed a true flag (meaning the piezoelectric sensor has something on it and there is a voltage across the sensor), then the indicator light will turn on. This function serves to show users which boxes are not currently occupied so they can put their phone in a box without trying the open a locked box.

4.2.6 Fingerprint Scanner

This unit handles all of the built in functions that allow the fingerprint scanner to run a scan, generate an image, store and transmit images into memory, match scans with images currently in memory, and then append or clear the memory of an image or character file when we no longer need it. This unit has built in functions that improve the security of the device and is integral to the locking and authentication of the device. The following is a list of variables and methods for the fingerprint scanner:

- **return_code:** This variable is for the return codes the fingerprint scanner uses when confirming that certain tasks have been completed. These return codes are used to debug any errors that may occur during runtime of different memory and scanning operations as well as clear other tasks to run without risk of failure.

- **image:** This variable is the image of the single print we will keep in memory for our purposes. We could use multiple image variables if we were using one device to scan prints for all boxes, but because we will have one scanner for each box, there is no need to keep multiple variable since each box will only be keyed to one print at a time. This image will be passed to Buffer1 when the Match() method is called.

- **ImageBuffer:** This variable is a buffer. When the fingerprint scanner initially scans and generates an image of a fingerprint, that image will be sent here. Depending on whether or not there is already data stored in the variable image, this data may either be passed to method Img2Tz() to be sent to image, or this data will be passed to match and be compared with the data in Buffer1.

- **Buffer1:** This variable is a copy of the data in image. The data in this variable will be compared to the data in Buffer2 to determine whether or not the two prints are a match when the method Match() is called.

- **Buffer2:** This variable is a copy of the data in ImageBuffer. The data in this variable will be compared to the data in Buffer1 to determine whether or not the two prints are a match when the method Match() is called.

- **GenImg():** This method will handle the processes required for the fingerprint scanning device to detect a finger, scan the finger, and then generate an image of the finger. The image generated will be sent to the ImageBuffer until that information is forwarded elsewhere. Upon completion of scan, this method will return a termination code. If the print is successfully scanned, a successful confirmation code will be sent. If there is no finger detected, the returned confirmation will be “can’t detect finger”.

- **Img2Tz(BufferID):** This method will pull the data stored in the ImageBuffer variable and generate a character file. That character file will then be stored in whichever buffer we designate. We will store the data in Buffer1. This function will return a confirmation code upon completion showing the results. Confirmation codes include success, error recieving package, and failure to generate character file.

- **Store(BufferID, PageID):** This method will be used to store the template of a fingerprint stored in Buffer1 or Buffer2 into a local library. We have not yet fully decided if we will need to use this function as the idea is to wipe the memory of any stored fingerprint images as soon as the device calls Unlock(). When this method completes, it will send a confirmation code telling us success, error receiving package, out of bounds, or error writing to flash.

- **Match():** This method will carry out precise matching of images stored in Buffer1 and Buffer2. This method will be very important for the purpose of verifying that the newly scanned fingerprint of the user matches with the one currently stored in Image (which is moved to Buffer1 to be used by this method). Upon completion of the operation, a confirmation code will be sent confirming positive for match, mismatch, and error receiving package.

- **Empty():** This is method the Unlock() method will call when it finishes in order to clear the memory of the of any print images currently stored. This method facilitates freeing up space for the next user to set their fingerprint in the device after the prior user retrieves their phone. When this method finishes, it will return a confirmation code denoting success, failure to clear library, or error receiving package.

4.3 Communication Protocols

This section will briefly cover the transmission protocol considerations for handling the inter-device communication we will need for out multiple devices. Many controllers come standard with accommodation for multiple different communication protocols. The transmission protocols we are considering for this device are Universal Asynchronous Receiver/Transmitter (UART), Universal Synchronous/Asynchronous Receiver/Transmitter (USART), Serial Peripheral Interface (SPI), and Inter-Integrated Circuit (I2C).

4.3.1 UART

The UART in a controller will take bytes of data, break it apart into bit, and then transmit those bits one at a time. Another UART at the destination will receive these bits of data and reassemble them into complete bytes. The UART is an asynchronous protocol, meaning that the sender is not needed to provide a clock signal to the receiver. Instead, the sender and receiver must agree on a timing parameter beforehand, and special bits are added to the transmission package to synchronize transmission. UART protocol will add on a start bit before the data bits. When the receiver sees the data bits, it will spend an equal amount of time on each bit. Unlike with I2C, the sender will never know if the receiver has seen or done anything as no acknowledgement is sent to the sender. Instead, a parity bit is sent by the sender to allow the receiver to do very simple error checking. After the parity bit, the package will then have a stop bit denoting the end of the transmission.

4.3.2 SPI

Serial Peripheral Interface (SPI) bus is a serial communication protocol for controlling and communicating with any electronic device that accepts a clocked serial stream of bits. SPI is typically used for short distance communications and is often found in embedded systems. SPI devices communicate in full-duplex, meaning that data can be transmitted in two directions at the same time. In SPI, full-duplex communication is accomplished using the master-slave architecture in which a single master control one or multiple slaves via a slave selection line. SPI is a communication protocol handled by a minimum of four signal lines:

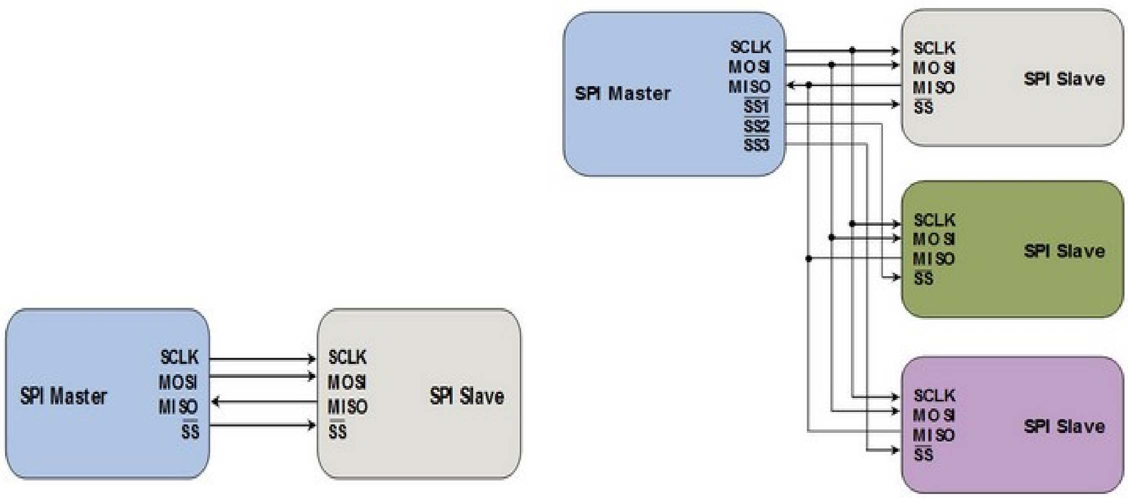
- A clock signal named SCLK: This signal is sent from the master unit to all slaves. All transmission signals in SPI communication are synchronous with the clock signal of the master unit.

- A slave select signal for each slave unit named SSn: This signal determines which slave unit the master unit is communicating with. For a single master, single slave system, there needs to be a minimum of four transmission lines (taking up four pins on the board). For each additional slave unit, we need to accommodate an additional slave select line.

- A data line connecting the master unit to the slave units named MOSI (Master Out-Slave In). This line is used to transmit information from the master unit to the slave unit.

- A data line connecting the slave units to the master unit named MISO (Master In-Slave Out). This line is used to transmit information from the slave units to the master unit.

The diagram below shows two SPI Bus topologies. The first topology is a single master connected to a single slave. A topology we can use for communicating between the box governor and the locking system controllers. The second figure is a single master, multiple slave configuration that we may see in the connection between the single unit governor and multiple box governor controllers.



Because SPI is both single master and synchronous, the master unit decides the clock rate for transmission. The Master and slaves must also agree on clock polarity (CPOL) and clock phase (CPHA) for transmission to happen. Aside from that, there really isnt any other defined requirements. SPI does not define a max data rate, addressing scheme, acknowlegement mechanism, or flow control.

One of the really good things about SPI is that it has very fast transmission speeds getting up to three times faster than Uart. It is also pretty cheap and not very computationally complex to set up. SPI is also super low power, making it very good for small embedded applications.

4.3.3 I2C

I2C is an official standard serial communication protocol. I2C is a synchronous protocol that only requires the use of two wires to transmit data. One of these lines is for the serial clock signal (called SCL), the other line is for the serial data (called SDA). I2C is capable of communicating between multiple slaves AND multiple masters and it does all of this communication on the same line. This protocol is capable of this because it doesn't need multiple slave select lines. Instead of multiple slave select lines, the protocol defines the following:

- 7-bit slave address: this 7-bit number denotes the address of a slave device. When a transmission is being made to the slave device, the slave device is selected via this address. 7-bit slave address means that there can be a possible 128 slave devices (much more than we need for our purposes).
- Data divided into 8-bit bytes.
- Control bits added to a transmission package for controlling start, end, direction, and an acknowledgement mechanism.

The data rate is small compared to SPI, usually set at 100kbps, 400kbps, and 3.4Mbps (Which is high speed mode). The Diagram below shows the basic connection of an I2C system.

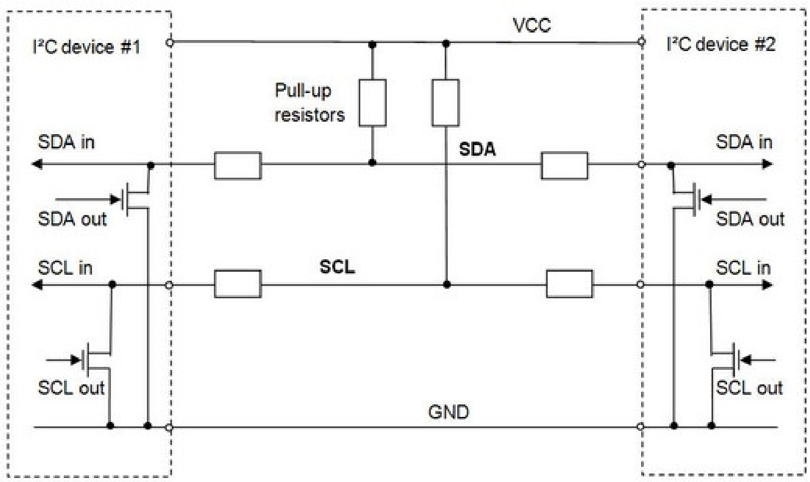


Figure 53 - Basic connection of an I2C system

Whichever IC initiates the data transfer is considered the master unit by I2C protocol. The master will send a START condition, and all slave units attached to the system will become active and start listening to the transmission bus for data. The master unit will then call the specific address it wants and the designated slave will then send an acknowledgement. The moment the master gets that acknowledgement signal, it will commence transmission. This is where one of I2C's biggest benefits is. The way the bus is implemented allows a master unit to simultaneously write and listen to the bus line, meaning any device can detect collisions and stop conditions can be issues as needed.

4.3.4 SPI vs I2C vs UART

UART and I2C are very similar to each other, the major difference between the two is that UART is an asynchronous protocol whereas I2C is a synchronous protocol. The UART protocol has to make modifications to a transmission package during transmission and the package sender is completely blind to what the receiver is doing during the transmission. In I2C, the master unit is capable of listening to the data bus during transmission, so it is capable of receiving acknowledgements from the slave units. Both protocols run on slow data rates, both only require two wires to properly connect transmitter and receiver, and both have formal standards. The advantage that I2C has over UART is that it is easier to program, the outcome of a transmission is known immediately due to acknowledgement signals, error recovery is much easier since the transmitter and receiver are sending diagnostics to each other, and there is usually a better real-time response in I2C systems. However, UART does not need requests to be target specific, and the transmission line can be idle. When it comes to bus topology, I2C is much easier to build the network and more space efficient than an SPI network. SPI is much faster at transmitting data though with implementations with data rates that go over 10Mbps. I2C draws more power than SPI, I2C offers functions for conflict handling that can be complicated to implement, but is still cheaper overall. Overall SPI’s functions are better suited for data streams while I2C is better suited for multi master register access applications.

For the purposes of our project, we will likely be using the I2C method to communicate between devices in the assembly, but use the SPI protocol to send information to the terminal for a viewer to see.

4.4 Physical Housing Design

The physical design for our charging remote alert notification station must be designed to accommodate quite a few things in a limited area. This means that care must be taken when designing to allow for ease of access, comfortable functionality and protection of the components. Below in Figure 54, you can see the proposed front view of our 3 chamber station. (Dashed lines represent the hidden interior.) All that will be on the front panel will be a fingerprint scanner, and some status indicating lights. Beyond the front panel, the inner chamber will have 2 microphones placed in the corners that will be used for sound detection. The reason for having one on both sides is to be able to verify the source of any sound that is detected and to be able to disregard noise that bleeds through past the insulation or otherwise.

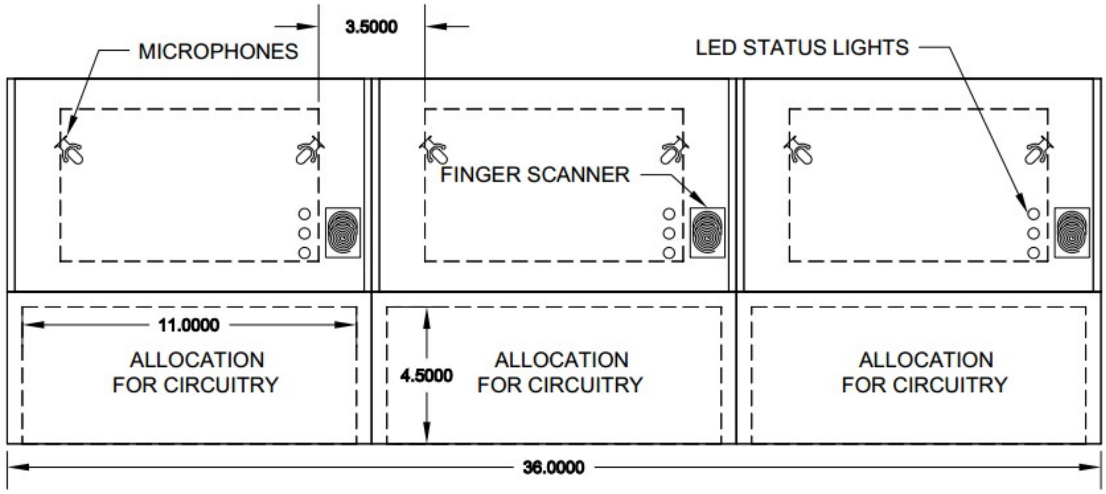


Figure 54 - Front View

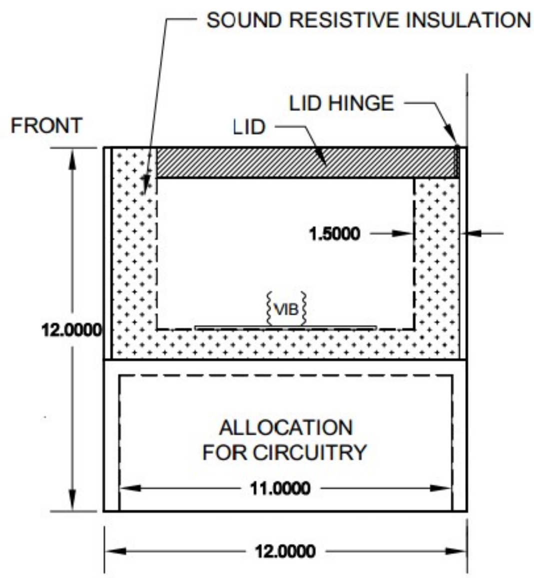


Figure 55 - Right Side Cut View

Each chamber will have a compartment underneath that will be spacious enough to house all of the necessary circuitry and components needed to implement our project design. The chambers themselves will be surrounded with ≈ 1.5 inches of insulation for isolation and damping purposes. As can be seen in the right side cut view in Figure 55, the lid of the container will open toward the back. When it opens, there will be a door contact to signal the controller to stop sensing. There will be a solenoid lock in the lid and when the lid is unlocked, there will be a spring to push the door open. This will allow for the solenoid to use the least amount of power as opposed to keeping the solenoid pulled in until the door is opened by the user. When the door is pressed closed, there will be a door contact to signal that the chamber is ready for sensing.

5.0 Testing Plan

This section will cover all of the testing plans and results for the different parts we have chosen to use within our design. We will show a schematic of the circuit we used for testing, and the measured results we obtained during those tests if applicable for the following parts:

5.1 Sound Sensor Testing

The testing method used for the sound sensor was building the circuit on a breadboard, and connecting it to an oscilloscope. Via the oscilloscope we could see the output for one microphone, two microphones and different scenarios where distance and compartment insulation affected the outcome. The microphone that we used is an electret microphone that is ideal in this kind of design. The circuit below shows an overview of the whole sound sensor circuit.

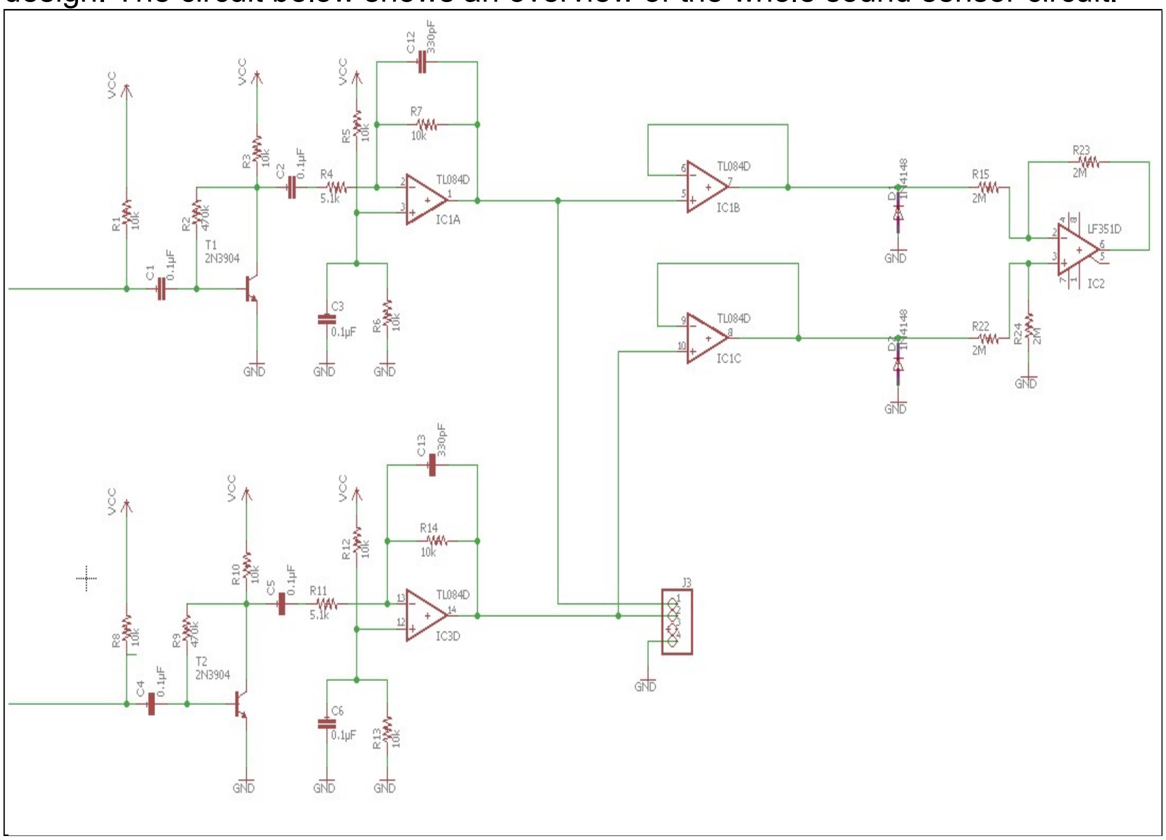


Figure 56 - Overall Microphone Sensors Schematic

The circuit above includes the circuit for the two microphones, the details on how they receive power, connect to the sensors, how they are grounded, and where the output goes. J1 represents the header that connects the sensors to the circuit, this way the sensors can easily be removed later during testing or actual design in case a sensor malfunctions. J2 represents the +5V power line and ground feeding into the circuit. With two bypass capacitors on the power supply C10 and C11, 10mF and .1mF respectively, if there's any noise coming in, the first capacitor will filter it out, if theres any high frequency noise, the other will filter it out. They will filter out any noise being picked up on the 5V line. Meanwhile all of the outputs connect to the J3 header that is going to be connected to the microcontroller. Using the header connectors makes it easier to later be able to be able to change parts that may need to be adjusted or changed. The following circuit will be analyzed in detail below. The schematic below shows the circuit for one of the microphones, where's the second microphone circuit is identical.

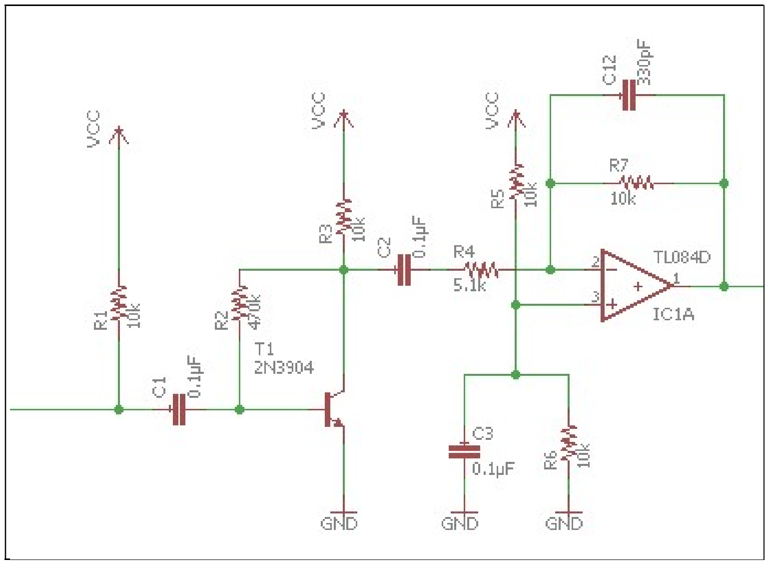


Figure 57 - Microphone1 Circuit

The microphone is connected to the beginning of the left side of the circuit. The circuit begins with R1, which is limiting the current so the microphone isn't instantly charged, so the microphone is acting like a capacitor, so R1 is basically biasing the microphone. Following that is the C1 capacitor. This capacitor is performing AC coupling to isolate the DC voltage which is useful because the DC component of a signal acts as a voltage offset, and removing it from the signal can make the signal stronger. This way the bias voltage of the microphone does not affect the bias voltage of the transistor. Now up to this point this circuit can be simply built and it will work, however for this application it is not enough. Now the circuit is connected to a NPN BJT for amplification. The BJT we are using is the 2n3904 is a NPN silicon transistor designed for general purpose amplifier and switching applications. A transistors steady state of operation depends a great deal on its base current, collector voltage, and collector current and therefore, if a transistor is to operate as a linear amplifier, it must be properly biased to have a suitable operating point. Establishing the correct operating point requires the proper selection of bias resistors and load resistors to provide the appropriate input current and collector voltage conditions. Transistor Biasing is important for setting a transistors DC operating voltage or current conditions to the correct level so that any AC input signal can be amplified correctly by the transistor. For this particular transistor, the emitter will be connected to ground, R2 is used to forward bias the transistor, which turns the transistor on, and R3 is used as the load resistor. R3 is connected to the collector side of the transistor and this will pull the voltage up but the transistor will bring it back down since the emitter is connected to the negative terminal. R3 has a negative feedback and is also biasing the transistor. Basically, following ohms law, if current changes changes, then voltage changes. If it draws more current, then voltage drops, if it draws less current, voltages goes up. Afterwards C2 does AC coupling, its purpose is to isolate the DC voltage so that only AC goes through. Then R4 is in series with it and both R4 and R7 set the gain of the op amp. It makes it act like a low pass filter so that only lets low frequencies go through. The OpAmp we used is a TL084 JFET-input operational amplifier, this opamp features high slew rates, low input bias and offset currents, and low offset-voltage and temperature coefficient. R4 is R feedback and R7 is R input. And the gain Is = Rf/Rinput if we want unity gain then we make them both 10k resistors. Its a starting point. Whatever comes in does not get amplified. If we need more amplification then we change Rinput. Say Rinput is 5.1k so itll give us a gain of 2, because 10/5.1=~2. So 1V amplitude peak to peak gives me 2V out. Calculations below show the gain of the op amp. R5 and R6 are acting as a voltage divider, this is to split the voltage from 5V, to 2.5V so to set the bias voltage of the op amp so that it sits at 2.5v. This is important because no negative voltage goes through the microcontroller, it only works from 0-5v. So if you have negative voltage, it goes in a halfwave rectifier and we lose all the negative signals so all we end up seeing are pulses. Also, the microcontroller requires an input between 1.8v-5.5v, at 2.5v the signal is in the correct range to be picked up by the microcontroller. This is why the voltage divider is useful, it brought our signal up so that we don't lose the negative parts. C3 is useful since the power supply will have noise, which will create open look gain, this is to make sure there's absolutely no noise. Noise from power supply is amplified by the open loop gain of op amp, which is bad and will distort our output signal. Then C12 is useful because the op amp could oscillate if I don't have a high frequency capacitor. This capacitor will eliminate any high frequencies. This is enough for the microphone to pick up and amplify an acoustic wave. The calculations below show how C12 was found. Basically we want anything above 50kHz to be filtered out at -3dB so that will be my Fc. Human hearing can hear up to 20kHz so we set the threshold to be a little more above that.

Gain of OpAmp: $Av = \frac{Rf}{Ri} = \frac{10k}{5.1k} = \sim 2$

Voltage divider: $Vout = Vin\ x\ \frac{R2}{R1+R2} = 5\ x\ \frac{10k}{10k+1} = 2.5V$

C12: $c = \frac{1}{2\pi RC}$, Now solving for C; $50k = \frac{1}{2\pi(10k)C}$ where C = 330pF

Now the circuit below shows the two microphones that we will be using in the compartment. The second circuit will be the same as the first circuit with the same values. They are both receiving the same input voltage and the second microphone also has an output of 2.5V. This was useful to test both microphones to see if they would have similar amplitudes depending on the distance.

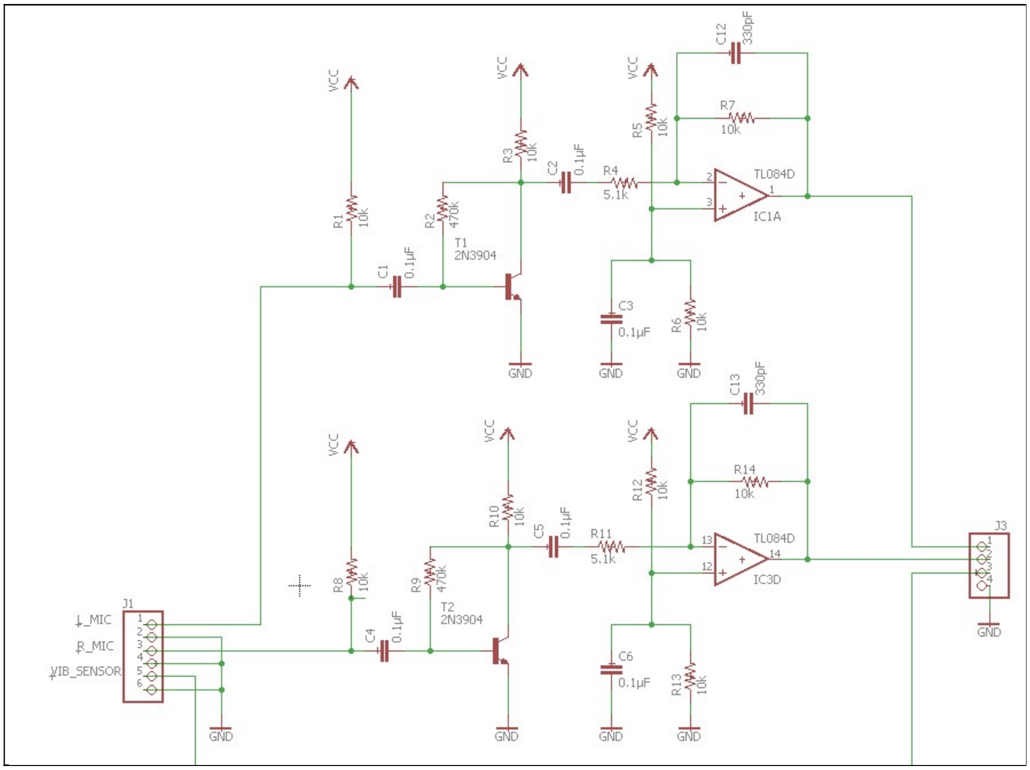


Figure 58 - Microphone1 and Microphone2 Circuit

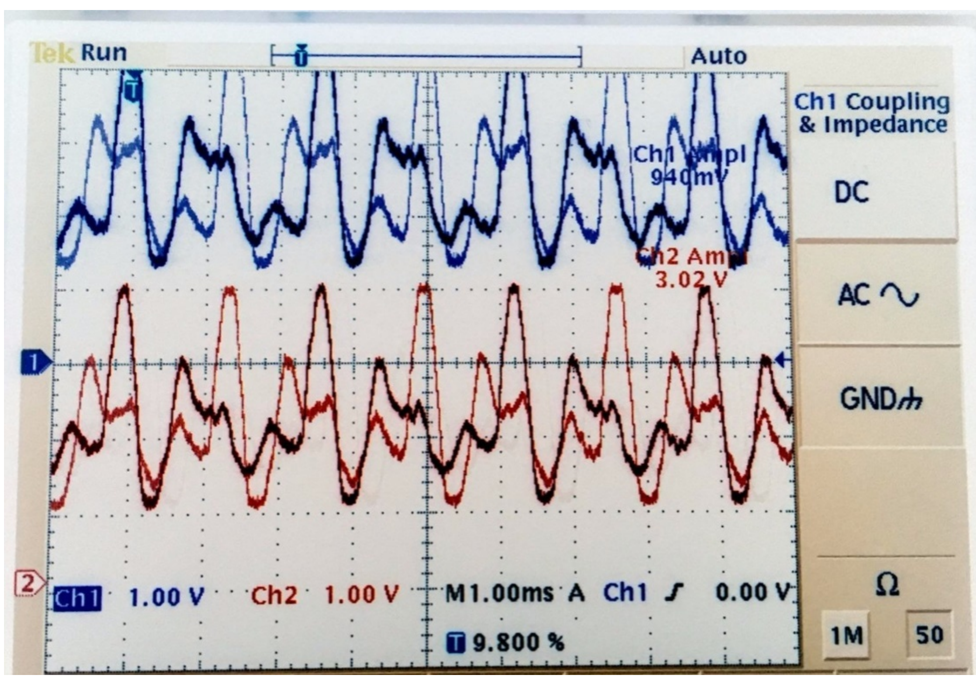


Figure 59 - Equal Amplitude DC

The above results show the DC voltage in microphone 1 and 2. Both microphones have an output of 2.5v after going through the opamp. They are showing the same signal as this test has both microphones close to eachother, this was only to test what their outputs would be in an ideal scenario.

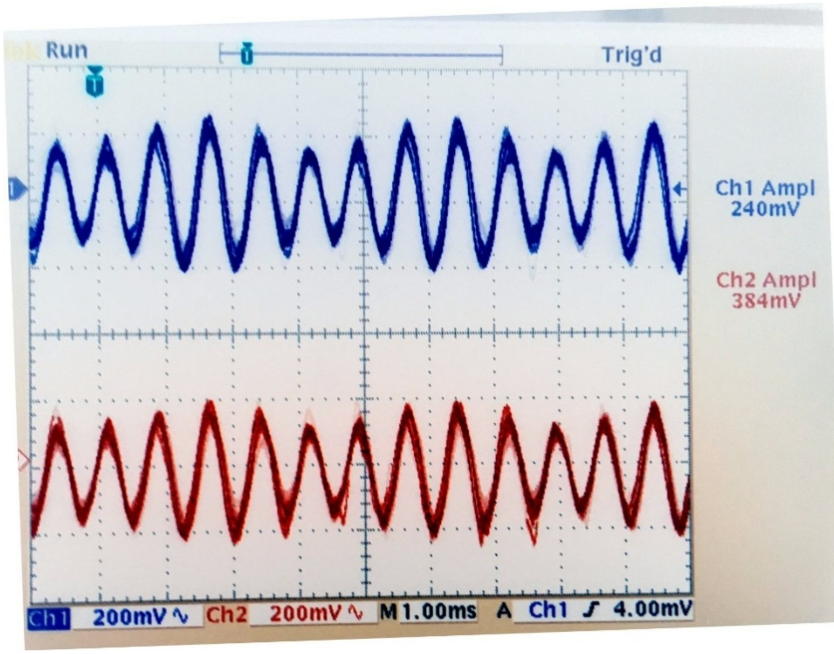


Figure 60 - Equal Amplitude AC

The above results show the AC voltage in microphone 1 and 2. Setting the scale to be at 200mV, the amplitude for both are around 300mV. This shows that at a 1kHz signal, both microphones will detect the same signal and have the same amplitude if they are both ideally only picking up the cell phone ring inside of their own compartment. By having the voltage divider the low signals did not get clipped, and by having the opamp then they acted as a low pass filters for only low signals to pass through.

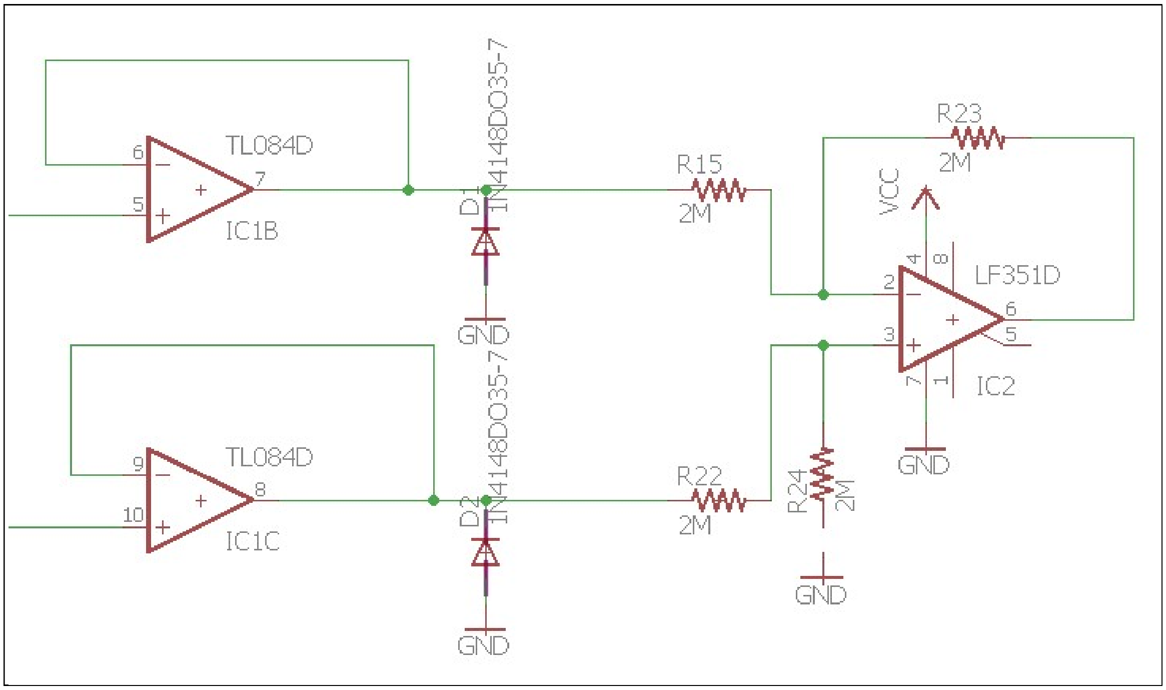


Figure 61 - Comparator

Now both outputs will go into a voltage follower, which is an op-amp circuit which has a voltage gain of 1. This means that the op amp does not provide any amplification to the signal. This is because the input impedance of the op amp is very high, giving effective isolation of the output from the signal source. You draw very little power from the signal source, avoiding “loading” effects. Then it goes through a diode so that current is only passing through one direction and finally it goes into a differential amplifier. The op amp we are using here is the LF351 which is a JFET input operational amplifier with an internally compensated input offset voltage. It provides wide bandwidth, low input bias currents and offset currents. The differential amplifier is a type of electronic amplifier that amplifies the difference between two input voltages but suppresses any voltage common to the two inputs. This is the comparator and it is useful because we need to be able to see the difference between the amplitudes in the two microphones, that way we can tell it to ignore certain the signal if there is a large difference. This is useful so that it won’t pick up the faint signal from another compartment and mistake the status of the phone in its own compartment.

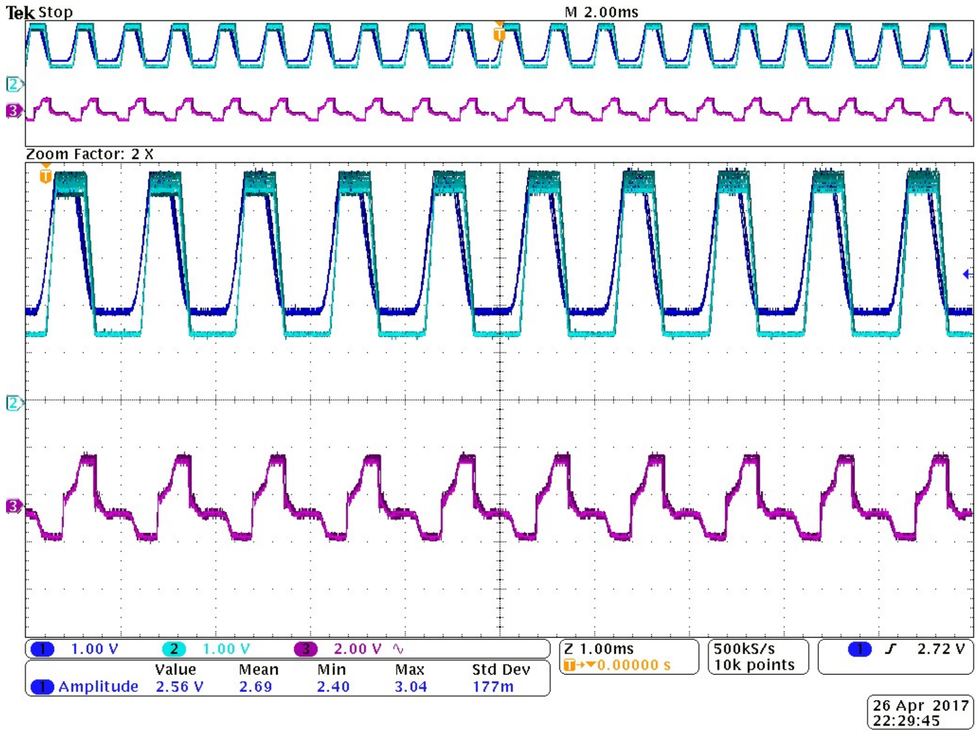


Figure 62 - Equal Amplitude Microphones with Comparator

The graph above shows the two microphones connected to a comparator and the result of it. The blue line is the first microphone, the green line is the second microphone and the purple is the comparator. The comparator can see that there is a difference in the signals when amplified. Both are being sampled at 1kHz and they both show similar amplitudes. The comparator is at a higher scale which is why the difference is exaggerated. In this scenario their difference should be minimal as both microphones are only listening to a sound inside of the same compartment. When a phone is ringing inside of the same compartment then the microphones will have a similar intensity which can only be achieved if the sound is equidistant from both microphones with no other disturbances in between.

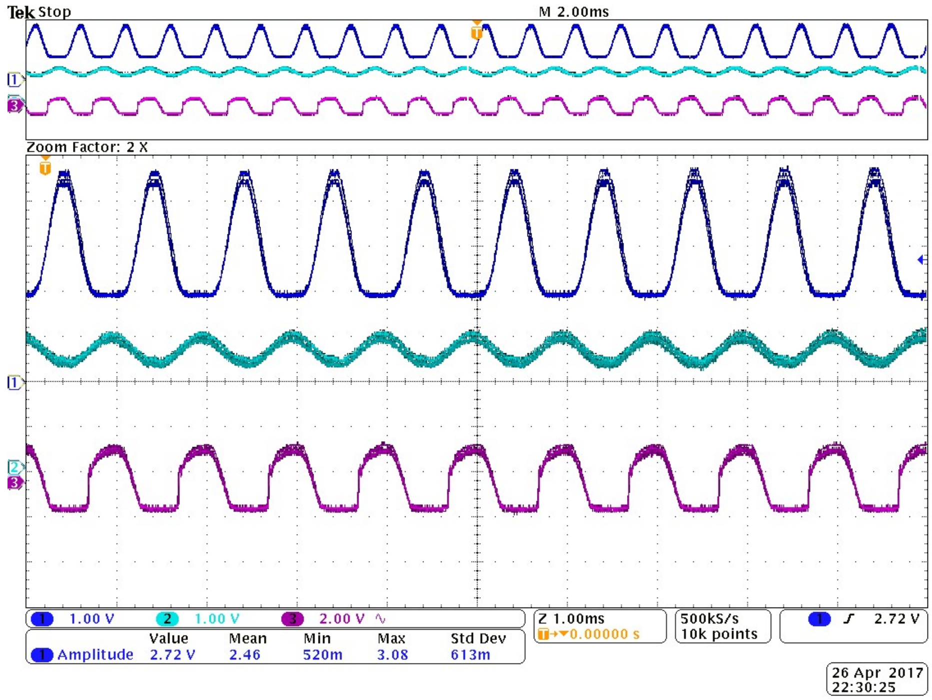


Figure 63 - Equal Amplitude Microphones in different compartments with Comparator

The final schematic takes into account if both microphones are inside of one compartment but picking up sound from the compartments next door. The other compartments have insulation blocking sound to go through, but as they are not perfect then signals next door can also be picked up and make the microphone give a false information. This is why the comparator is useful. In this case microphone 1 is the blue line and it is picking up sound from the compartment next door, meanwhile microphone 2 which is the green line is only picking up a faint sound from the compartment next door. The comparator shows a drastic change between the two signals which can then be used by the microcontroller to understand that the phone in the first compartment cannot be ringing or else both microphones would have a much similar output as seen in the previous graph.

5.2 Vibration Sensor Testing

The testing method used for the vibration sensor was building the circuit on a breadboard, and connecting it to an oscilloscope. Via the oscilloscope we could see the output for the sensor. The sensor that best fits our project is the Goedrum Piezo Disc. It is a 35mm wide brass piezoelectric disc that is ideal to be used as touch sensors. We originally wanted a piezoelectric sensor since they have high sensitivity when converting sound pressure into voltage. This particular sensor is thin and light weight, which is important since it'll be sitting of a box with several other components, so it needs to be thin or everything won't fit correctly. They only require a low power consumption as advertised, only needed 5V to operate. They are also known for providing clear sound waves and no noise. Testing was done by placing a phone on top of the sensor and making it vibrate. This way the phone sits on top of the sensor, not only acknowledging

that there is a presence of a cell phone unit, but also capable of picking up vibrations when someone is calling. Next we tried using some of the insulation components to simulate how it would be like when multiple units are attached next to eachother. We placed it in a proper housing for it, with insulation material all around and surprisingly the sensor was able to detect even through thick layers of insulation. On one side this is perfect for our project since the sensor needs to be sensitive to all vibrations.
The circuit below shows an overview of the whole vibration sensor circuit.

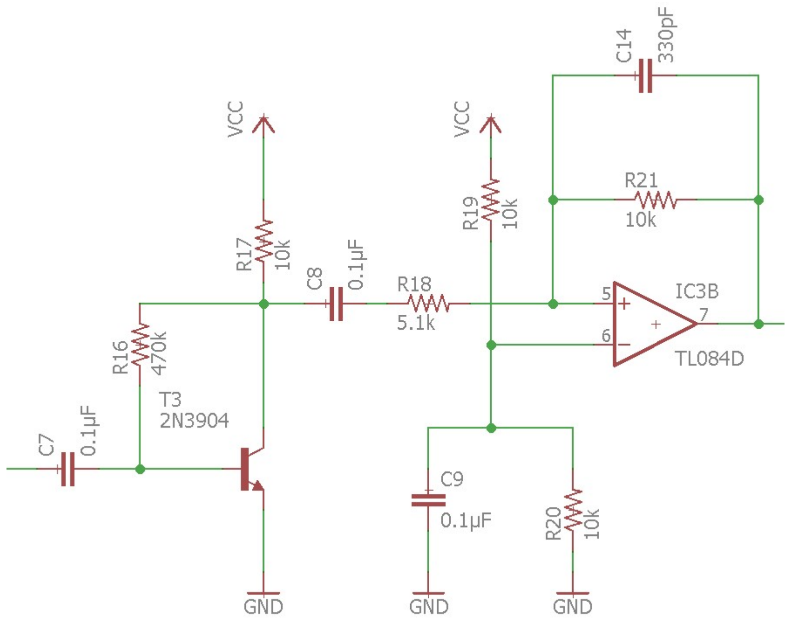


Figure 64 - Vibration Sensor Circuit

The vibration sensor circuit is similar to the microphone sensor circuit. It is connected to the beginning of the left side of the circuit. The circuit begins with the C1 capacitor where it is performing AC coupling to isolate the DC voltage which is useful because the DC component of a signal acts as a voltage offset, and removing it from the signal can make the signal stronger. This way the bias voltage of the microphone does not affect the bias voltage of the transistor. Now up to this point this circuit can be simply built and it will work, however for this application it is not enough. Now the circuit is connected to a NPN BJT for amplification. The BJT we are using is the 2n3904 is a NPN silicon transistor designed for general purpose amplifier and switching applications. A transistors steady state of operation depends a great deal on its base current, collector voltage, and collector current and therefore, if a transistor is to operate as a linear amplifier, it must be properly biased to have a suitable operating point. Establishing the correct operating point requires the proper selection of bias resistors and load resistors to provide the appropriate input current and collector voltage conditions. Transistor Biasing is important for setting a transistors DC operating voltage or current conditions to the correct level so that any AC input signal can be amplified correctly by the transistor. For this particular transistor, the emitter will be connected to ground, R2 is used to forward bias the transistor, which turns the transistor on, and R3 is used as the load resistor. R3 is connected to the collector side of the transistor and this will pull the voltage up but the transistor will bring it back down since the emitter is connected to the negative terminal. R3 has a negative feedback and is also biasing the transistor. Basically, following ohms law, if current changes changes, then voltage changes. If it draws more current, then voltage drops, if it draws less current, voltages goes up. Afterwards C2 does AC coupling, its purpose is to isolate the DC voltage so that only AC goes through. Then R4 is in series with it and both R4 and R7 set the gain of the op amp. It makes it act like a low pass filter so that only lets low frequencies go through. The OpAmp we used is a TL084 JFET-input operational amplifier, this opamp features high slew rates, low input bias and offset currents, and low offset-voltage and temperature coefficient. R4 is R feedback and R7 is R input. And the gain Is = Rf/Rinput if we want unity gain then we make them both 10k resistors. Its a starting point. Whatever comes in does not get amplified. If we need more amplification then we change Rinput. Say Rinput is 5.1k so itll give us a gain of 2, because 10/5.1=~2. So 1V amplitude peak to peak gives me 2V out. Calculations below show the gain of the op amp. R5 and R6 are acting as a voltage divider, this is to split the voltage from 5V, to 2.5V so to set the bias voltage of the op amp so that it sits at 2.5v. This is important because no negative voltage goes through the microcontroller, it only works from 0-5v. So if you have negative voltage, it goes in a halfwave rectifier and we lose all the negative signals so all we end up seeing are pulses. Also, the microcontroller requires an input between 1.8v-5.5v, at 2.5v the signal is in the correct range to be picked up by the microcontroller. This is why the voltage divider is useful, it brought our signal up so that we don’t lose the negative parts. C3 is useful since the power supply will have noise, which will create open look gain, this is to make sure there’s absolutely no noise. Noise from power supply is amplified by the open loop gain of op amp, which is bad and will distort our output signal. Then C12 is useful because the op amp could oscillate if I don’t have a high frequency capacitor. This capacitor will eliminate any high frequencies. This is enough for the microphone to pick up and amplify an acoustic wave. The calculations below show how C12 was found. Basically we want anything above 50kHz to be filtered out at -3dB so that will be my Fc. Human hearing can hear up to 20kHz so we set the threshold to be a little more above that. The circuit will then be connected to header to receive a +5V input and ground, another header that connects to the vibration sensor itself, and a last header that connects the output to the microcontroller for the information to be sent.

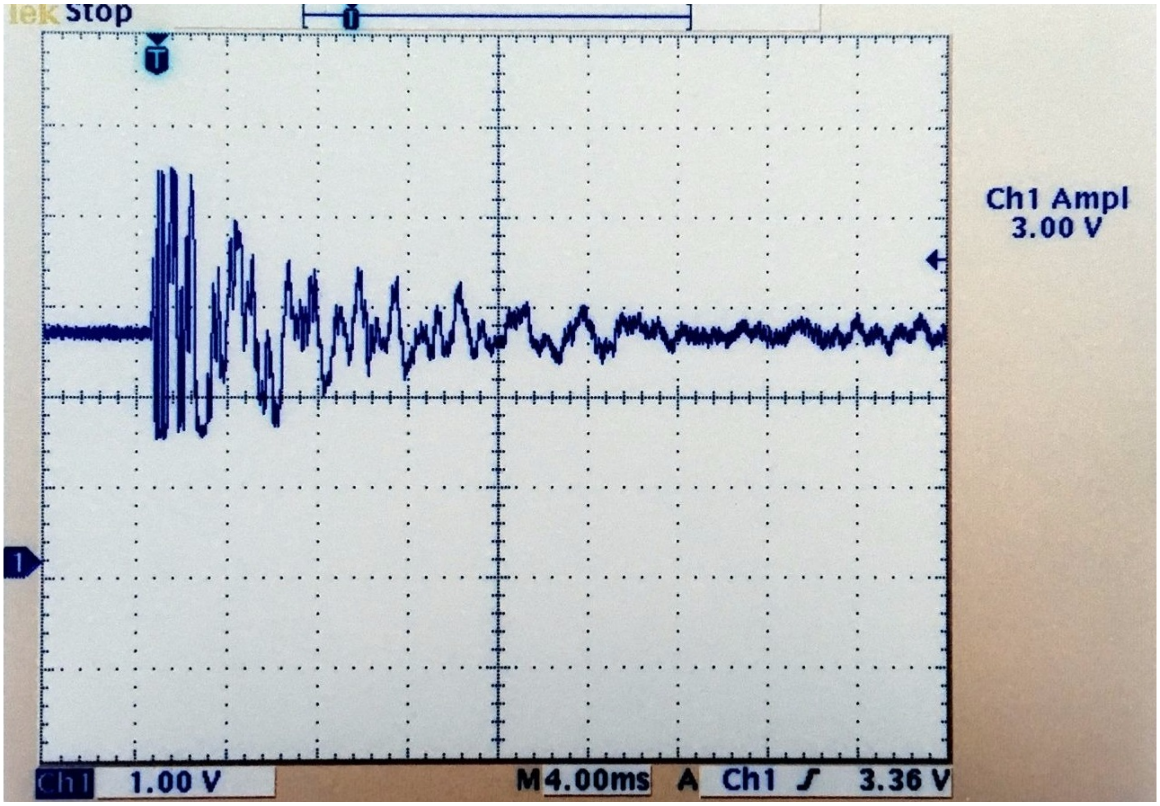


Figure 65 - Vibration Sensor Output

As shown above, claims that this sensor reduced noise and provided a clear signal proved to be true. Each oscillation represents one full vibration from the cell phone. It also looks like one vibration takes about 0.30s to start and stop, with several repetitions until the user is alarmed that their cell phone has a notification. The amplitude is at 3V since the signal was amplified by the op amp with a gain of 3. This will be a high enough amplitude for the microcontroller to detect and be able to process the information so that it can send a message that the phone is vibrating inside of the unit. This sensor proved to be sensitive enough for our purposes, however as it is very sensitive then the compartment insulation will take care of making sure that it doesn't detect any other vibrations nearby. However since this sensor works via pressure, then it will only detect the vibration of what is placed on top of it.

5.3 Security Controller Testing

In this section we will cover the testing plan and procedures that were used to test the different parts of the security subsystem in our project. The testing of the ATmega328 with all of the parts that will be used has not been performed but the main circuit design can be found in the Hardware section of the project design. This will cover the each of the other parts completely isolated from one another. In our project design the controller will be sending and receiving input from the fingerprint sensor, and it will control indicator lights on the outside of the container that will let the user know if the container has power, if it is already occupied, or if the fingerprint sensor is active. If the fingerprint successfully matches the registered print, the controller will actuate the lock allowing the contents of the locker to be retrieved. It will also communicate with the sensing controller with a single pin to signal whether or not it should be actively monitoring the contents. Once the chamber is opened, all monitoring should cease until the container is shut again. Whether or not the chamber is open will be monitored with a reed switch by the controller as well.

5.3.1 Solenoid Lock Testing

Our project will be using a normally open 12 volt pull-in solenoid to lock the chambers. They way this will work is that it will be activated by the ATMega328 security microcontroller. The output of the microcontroller pin will be the same as the input voltage VCC which is 5 V. We will use a 'High" output from the microcontroller as the control input into the "gate" of a FQP30N06 N-channel Mosfet transistor. This Mosfet was chosen to minimize the amount of current draw on the pin. According to the datasheet for the FQP30N06 [22], the Mosfet has a minimum ON threshold voltage between 1 volt and 2.5 volt and can operate at up to 10V which allows it to be used with either a 3.3 volt or 5 volt that are usually used for microcontrollers. The circuit used for initial testing is shown in Figure 66. The solenoid will be on the source side of the transistor with a 12 V input on the collector side. A diode will be placed in parallel with the solenoid to mitigate the transient voltage created by the magnetic coil in the solenoid. To test the solenoid, we will build the circuit and use a 5 volt source with a push button in place of the microcontroller.

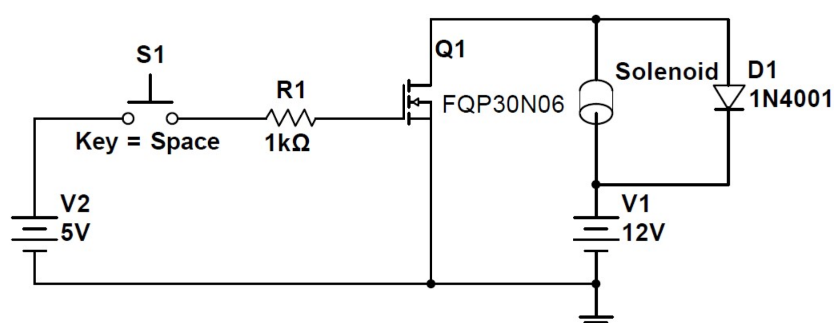


Figure 66 - Solenoid Lock Test Circuit

A digital multimeter was used to test the current through the solenoid and the testing of this circuit verified that the solenoid matches its specification in that it indeed only draws 300mA when a 12V source is applied. We measured it to be 303 mA at 12 volts which is only a 1% error. The MOSFET only pulled about .25mA which also falls in line with its specifications.

5.3.2 Fingerprint Scanner Testing

The other main part of our security subsystem is the integration of our fingerprint scanner. There are quite a few functions that will all need to be handled and controlled by the controller. For testing purposes, there will need to be a way to

set a person's fingerprint, a way to reset the registered fingerprints, a way of indicating the success or failure of a secondary fingerprint, and a way to verify that there is power to the sensor. In the final design the all of the indications and signals will go will be sent and received by the locking controller. But, for the purposes of testing and verifying the functionality of the sensor we will be using the K202 fingerprint control board which comes from the same manufacturer as the fingerprint sensor and is designed specifically for the sensor. This is only being used for testing purposes.
The K202 fingerprint control board will be connected to the fingerprint scanner logic board via a 4-wire UART connection. The scanner logic board shown in Figure 67 is connected to the fingerprint scanner with a 9-pin ribbon cable. The scanner logic board is responsible for reading the raw input from the fingerprint scanner as well as storage of the fingerprints, and comparing. The fingerprint control board as shown in Figure 68 is used to indicate that the system is in a working state by slowly flashing an LED that is used as an indicator light. There are two buttons on the control board that will be replaced with signals from the security microcontroller.

To register a fingerprint to the scanner logic board memory with the control board, you press the SET button to initialize a register state. With the system in register state, the indicator light will flash fast and the fingerprint can be registered continuously while in register state. Once the fingerprint is done being added, you can exit the register state by waiting 5 seconds or by pressing the SET button. To clear the logic board memory back to the default factory setup with the control board, you press the RESET button until hear an audible tone from the onboard buzzer which will be maintained until the button is released. Hearing a long audible beep means that extends beyond the release of the button indicates that the operation was successful.

To verify a fingerprint input with the control board you leave the system in its normal state (not register state) and attempt to read a new fingerprint. If it matches or the door button a normally closed contact labeled "door" is actuated and kept open for 5 seconds before closing again. There is also a motor contact interface that outputs DC 5V for half a seconds, stops for 5 seconds, then outputs a minus voltage for half a second, effectively returning it back to the start position. While the control board works as indicated, in our project design, we will instead be using the match signal to close a normally open contact as the control wire into the Mosfet of the lock circuit.

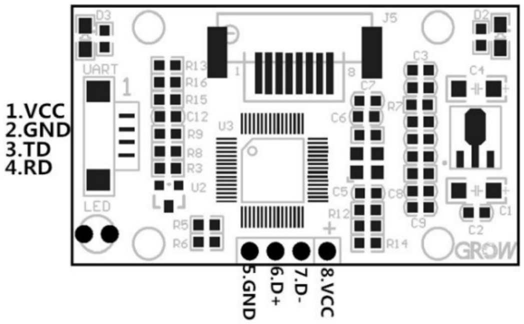


Figure 67 - Scanner Logic Board

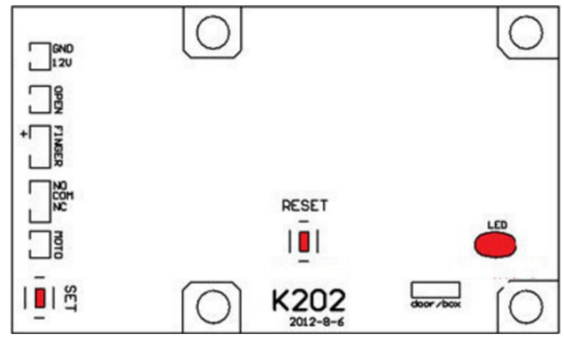


Figure 68 - Fingerprint Control Board

5.3.3 Event and Collision Detector / Basic Network

The following schematic shows a simple edge detection circuit as well as a simple networking scheme powered by the Beaglebone Black controller. (Let it be known that the current schematic is not entirely accurate as the software used to draw it does not currently have the specific processor used in the Beaglebone. We will correct this in the future.) The purpose for this edge detector will be realized when the whole system comes together. As the slave wired controllers attached to the Beaglebone controller detect disturbances inside the observation chambers, they will send flag signals. Those flags will be of a certain voltage level less than 1.8 volts for the Beaglebone controller to actually recognize that the flag it is receiving is valid and can throw an interrupt in the programming. The circuit only takes care of the voltage level of the flag signal since the output of the slave controllers is higher than 1.8 volts. The processor itself houses the programming that handles all of the timings, transmission of messages, and any and all return flags to alert the slave controllers to change a course of action. When the whole system comes together, the slave controllers will also have the other sensor circuits as well as other necessary functional components such as the print scanner and locking circuits attached as well.

For the purpose of testing the basic concept, we only paralleled two auxiliary devices with the Beaglebone controller. Each of those devices currently has one analog line attached to the analog inputs of the Beaglebone. Because the output on the auxiliary controllers, which is taken from the cathodes of the green and red LED's, is approximately 2 volts, we have to reduce that voltage to less than 1.8 volts. There is a voltage splitting component attached to the output of the auxiliary devices that we take the analog input for the Beaglebone controller from. The voltage splitter drops the input voltage into the Beaglebone analog input from 2 volts to a maximum 1.6 volts. After that, the Beaglebone had one of its pulse width modulation (PWM) pins set up to power a white LED. This LED serves as a physical indicator that the Beaglebone is throwing an interrupt. The system was set up so that at default state, the red and green LED's are at constant output HIGH until the built in button is pressed. This button acts as our "disturbance" for this test, and when it is pressed, the associated LED (the controller with the shining red LED controls the red LED on the breadboard, and the controller with the shining green LED controls the green LED on the breadboard) will toggle to output LOW. When one of these "disturbances" takes place, the Beaglebone will read the analog value across the voltage splitter of the individual auxiliary controller, and if it reads low, it will toggle the white LED to flash in a certain sequence shown below.

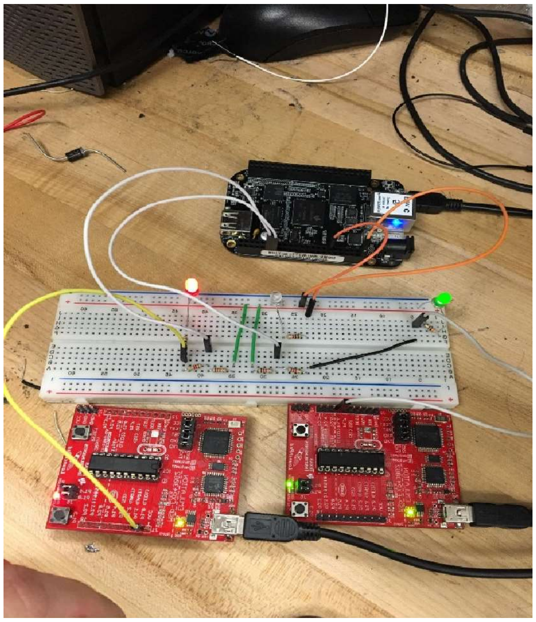


Figure 69 - - No Disturbance

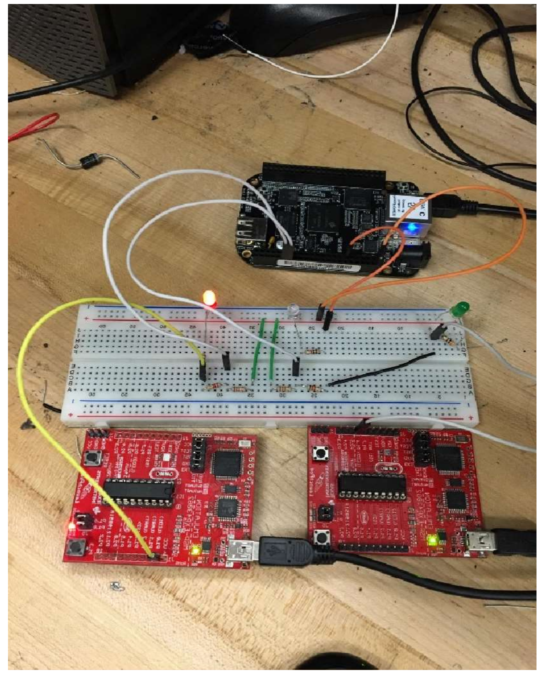


Figure 71 - - Disturbance Green

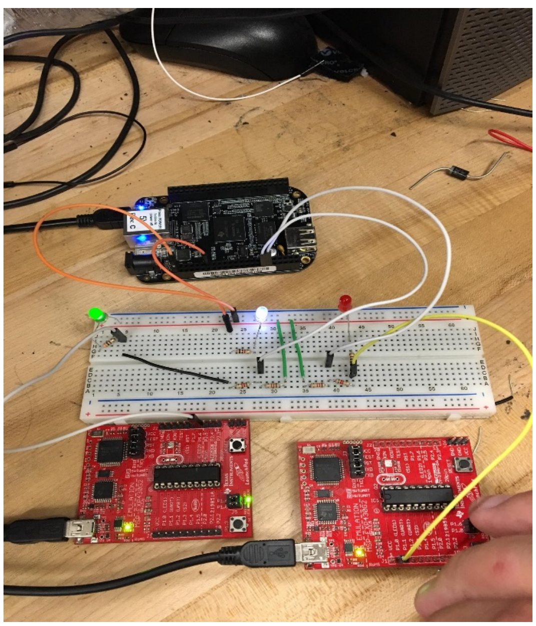


Figure 70- - Disturbance : RED

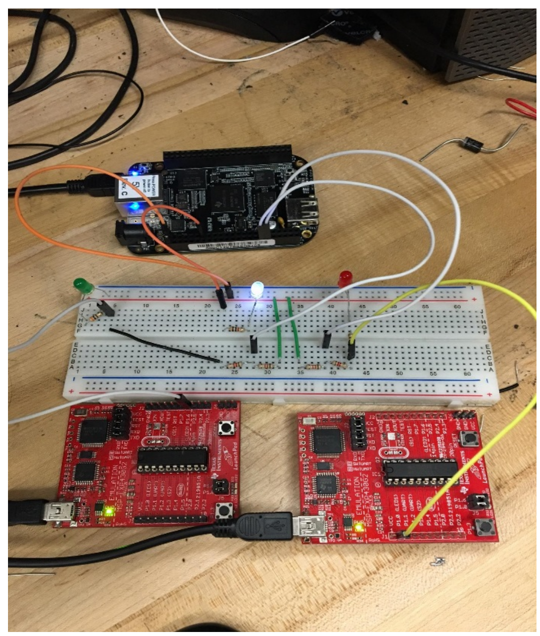


Figure 72 - - Disturbance : Race Condition

The images above don't really show it that well, but the white LED is showing a distinct difference between disturbance types. When both of the auxiliary controllers are reading no disturbance as shown in the first figure, the white indicator LED attached to the Beaglebone is set to output LOW, meaning it doesn't light. When either the red controller or the green controller are reading a disturbance, the white indicator LED will repeatedly toggle between output LOW and output HIGH every 100ms. When both auxiliary controllers are reading a disturbance, the white indicator LED will maintain a solid output HIGH without any toggling. This is a race condition and it is very important to us.

Our device will be reading all of these flags and sending out appropriate messages. If one observation chamber registers a valid disturbance at a time, then the Beaglebone has an easier job of just reading the flag, throwing the appropriate interrupt, and then sending a message. However, if multiple observation chambers register proper disturbances in close enough succession to each other, then we will be having multiple auxiliary controllers demanding certain resources of the Beaglebone at the same time, which can cause havoc in the system. When the Beaglebone detects this possible race condition, we need to throw a very specific interrupt that handles these simultaneous events and prevent collisions. At this current point in the testing, the code for this collision prevention has not yet been written. The code used in this test only detects the possibility of a race condition, but since there is no actual conflict over resources just yet, the system does not take measures to avoid it.

5.4 Component Testing

The level shifter works on the premise of saturation. When the higher voltage goes higher than the lower voltages maximum limit, it saturates and flattens out at that maximum voltage. This is very useful when using I2C, as I2C is a digitally encoded communication. It is important that the circuit does this, and doesn't noticeably slew. The Level shifter we plan to use is shown below in Figure 73.

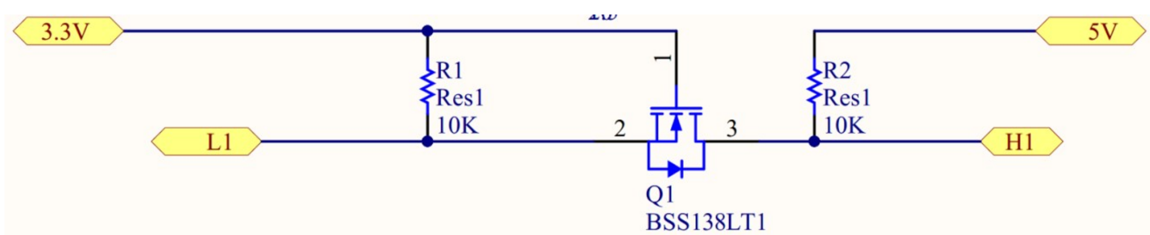


Figure 73 - Level Shifter

5.4.1 Methodology for testing

To test the circuit before accidentally blowing our controllers, we hooked it up to a 3.3V and 5V pull-up supply, and then used a function generator to supply a square wave input to the input pin. We repeated this step and all measurements with an amplitude of 5V to the H1 pin, and an amplitude of 3.3V to the L1 pin. The Oscilloscope results are shown below. The level shifter below in Figure 73 with reference voltages of 5V and 3.3V and a 5V square wave applied to the H1(Dark Blue) pin and the L1(Light blue pin) measured for consistency.]

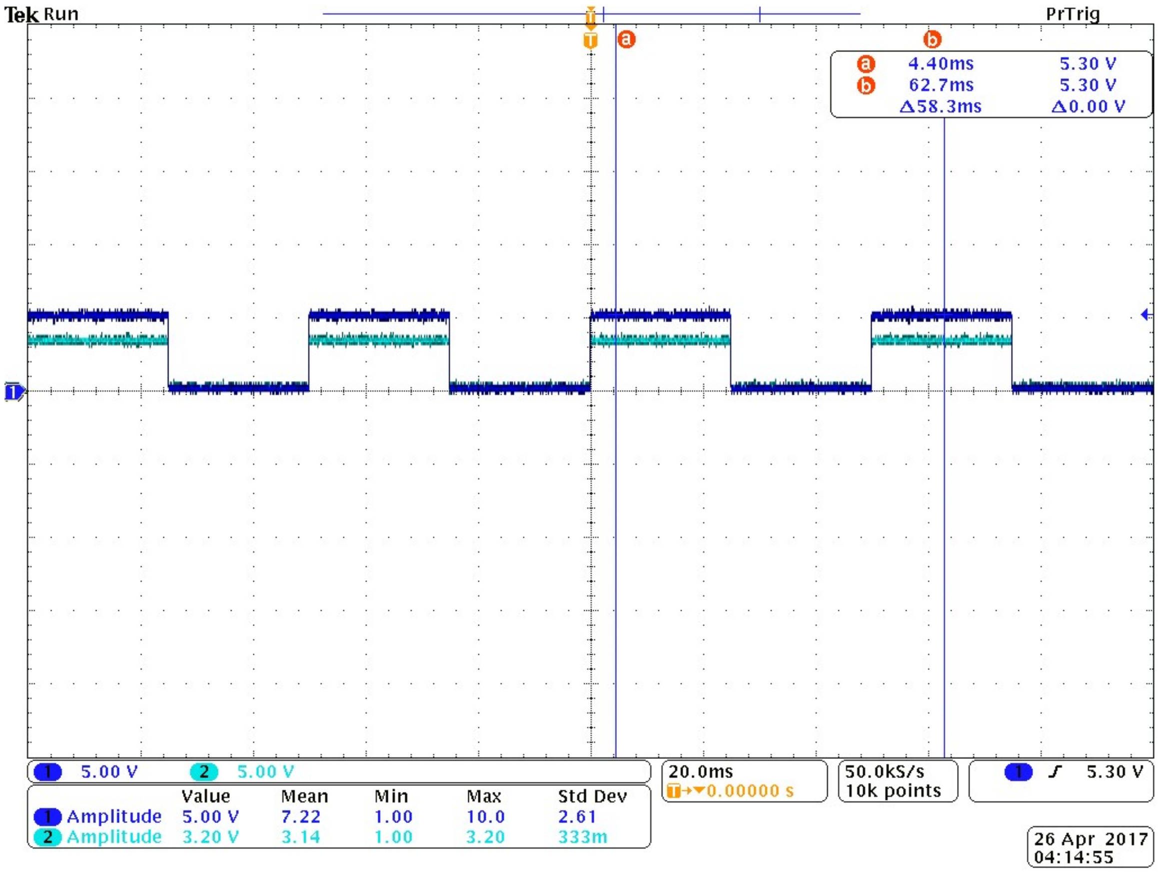


Figure 74 - The level shifter with reference voltages

When applying the 5V square wave to the pin, the output was exactly as desired, being comfortably under 3.3V while being close enough to ensure being considered on. It was consistent, and had an identical transition time to the input of the signal.

The same circuit is attempted again in Figure 75, with a voltage amplitude applied to the opposite side. Unfortunately, there was an issue with lab supply, which overshot the reference voltages. The Level shifter with the BSS138 mosfet worked perfectly for all levels and desired shifts with only reference voltages required

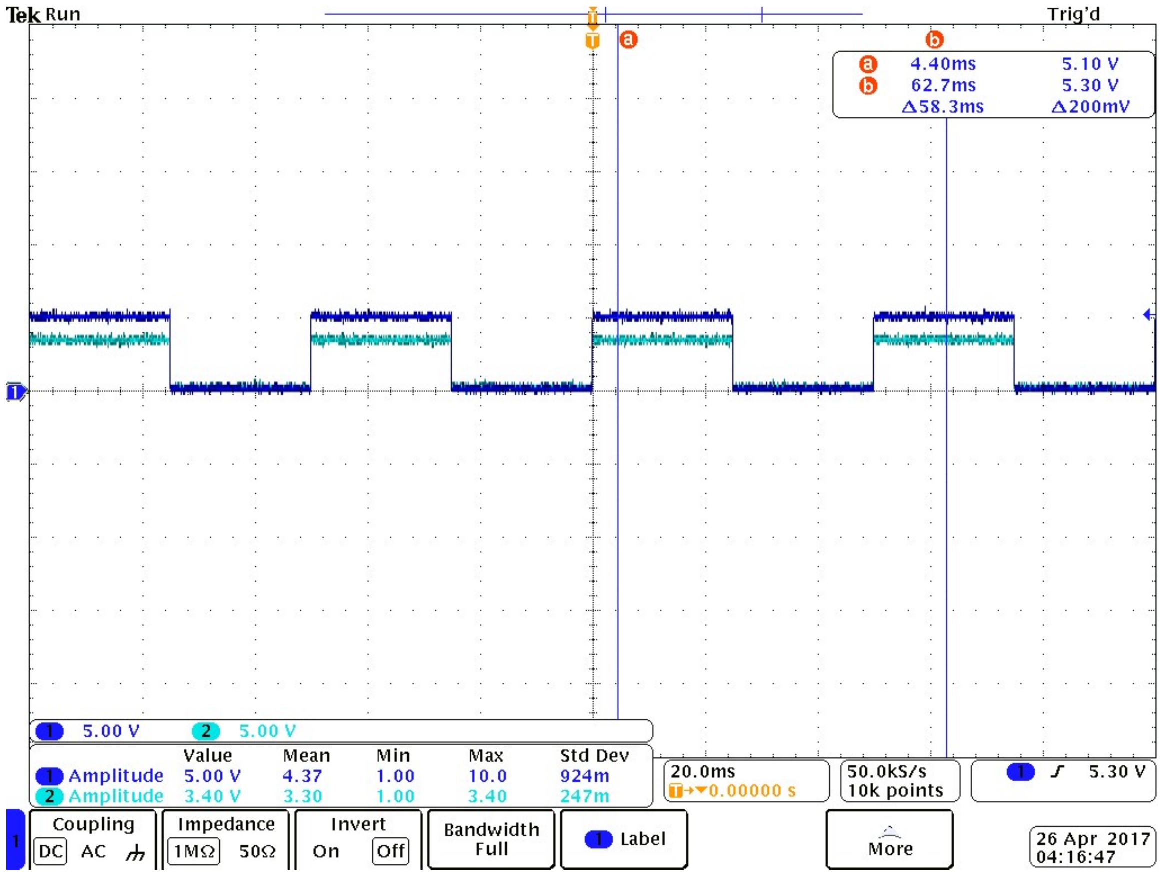


Figure 75 - Level Shifter Error

5.4.2 Voltage Regulator

To ensure the voltage regulator had the desired output, with appropriate tolerances, we tested the regulator circuit on its own. The circuit was set up, and tested with values that approximate the output. In most of our future testing involving 5V inputs, including those of the microphone sensing, we used the Rail regulator circuit with large Input, and Output Capacitors, and voltage buffers to ensure a smooth enough output to prevent biasing issues. Future Circuits will be fine tuned with the appropriate capacitors for an effective discharge and smoothing, however, those were not on hand.

Below shown in Figure 76, is the oscilloscope output for the Rail Regulator circuit. The Regulated 5V is in light blue, and the unregulated 12V input is in dark blue. The 5V output on the lower end of the swing can go as low as 4.7V which is within operating capacity of all components. When tested under load the signal shifts up by about .5V, leaving it oscillating at just above 5V.

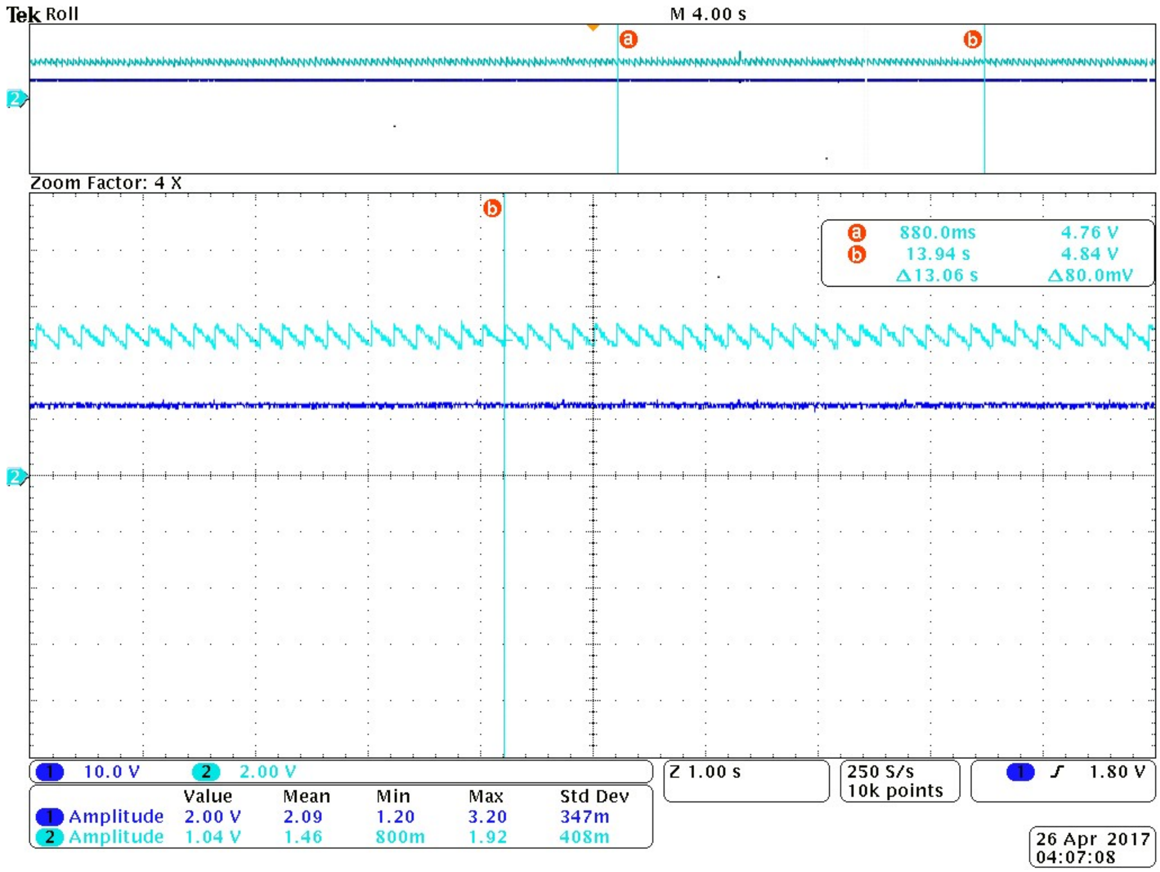


Figure 76 - Rail Regulator circuit Output

5.4.3 Level shifter with 5V Switching Regulator

After verifying both circuits, putting them together proved to be nontrivial. There were a decent number of input capacitors necessary for the level shifter, and the slew rate of the op amp for the voltage follower was much too low for any reasonable testing.

Below in Figure 77 and subsequently Figure 78 we have tested the BSS138 level shifter with a switching regulator. 3.3V in light blue, and 5V in dark blue. Test of 3.3V square wave inputted on the L1 side as well as test of 5V square wave inputted on the H1 side.

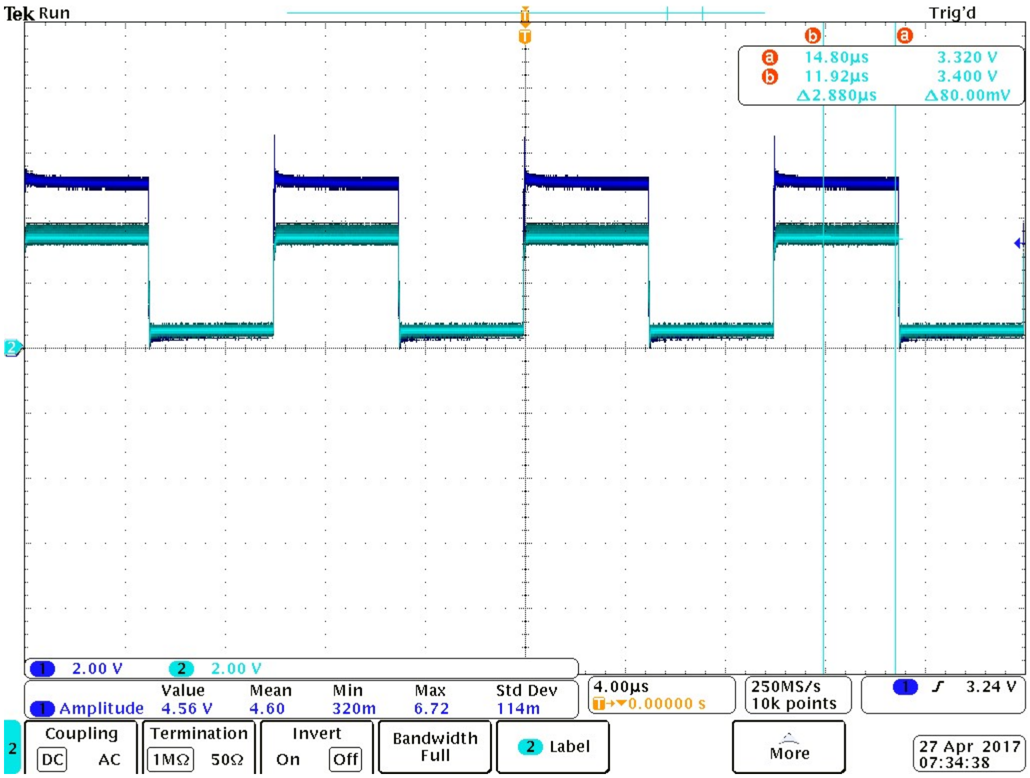


Figure 77 - Tested BSS138 level shifter with 3.3V Square Wave

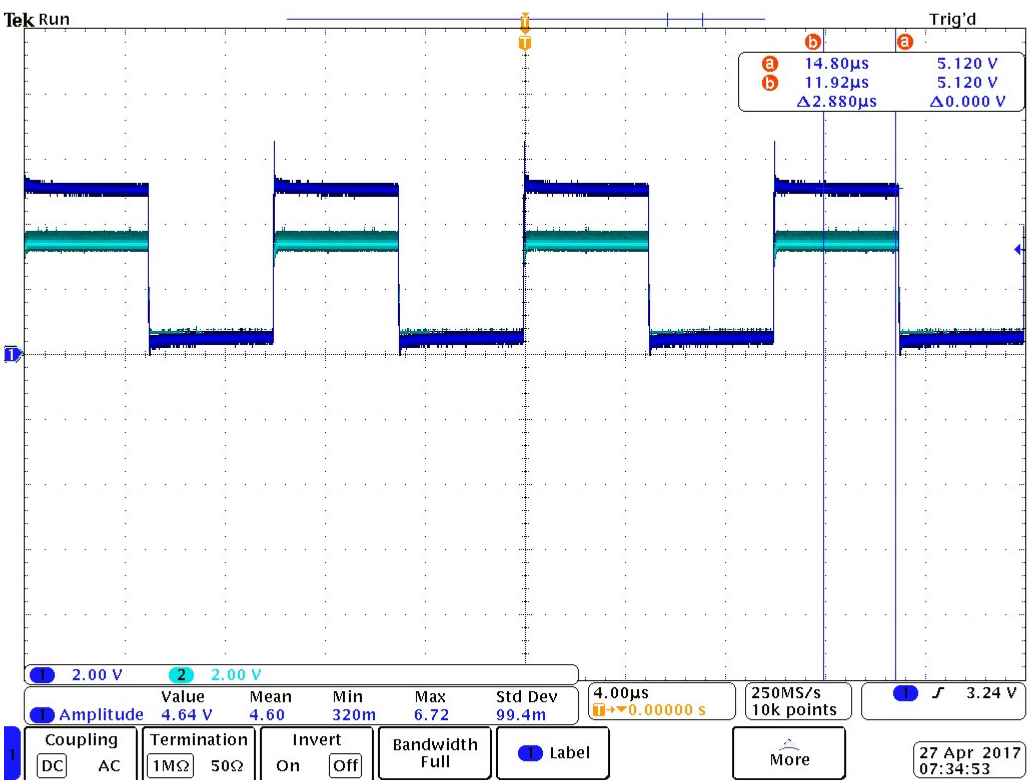


Figure 78 - Tested BSS138 level shifter with 5V Square Wave

The largest consideration was fine tuning the circuit for the 5V rail regulator. Since the regulator design was tuned for a significantly current output, the voltage levels are going to be a little off base from what the final circuit is going to be, but the behavior of the output and signals were sufficient to validate its possibility.

5.4.4 PCA9306

The PCA9306 was also tested using the 5V rail regulator and a 3.3V LDO. The PCA9306 worked really well when it was working, but under the situations where it wasn't working too well, it had a rather large margin of error. For the testing of this component, it was necessary to use a dedicated lab DC power supply, for the sake of ensuring its validity. If this component is going to be used, there will need to be a lot more thought put into smoothing out the regulator output.

For the testing, the 3.3V supply was connected to vref1, and the 5V supply was passed through a 200k ohm resistor into the enable and vref2 pin. From this point, there was a signal generated on the respective SCL pin, and the output on the opposite side was probed. This allowed for us to get a simple sense of how it handles high frequencies (100KHz for all tests) and the shifting capacity.

Below in Figure 77 and subsequently Figure 78 we have tested the BSS138 level shifter with a switching regulator. 3.3V in light blue, and 5V in dark blue. Test of 3.3V square wave inputted on the L1 side as well as test of 5V square wave inputted on the H1 side.

In Figure 79 and subsequently Figure 80, we have tested the PCA9306 level shifter with a switching regulator. 3.3V in light blue, and 5V in dark blue. Test of 3.3V square wave inputted on the L1 side as well as test of 5V square wave inputted on the Vref side.

The results of the PCA9306 were not very satisfactory, however, the circuit was very briefly looked into. Moving forward into the implementation phase, it will be more deeply considered and tested.

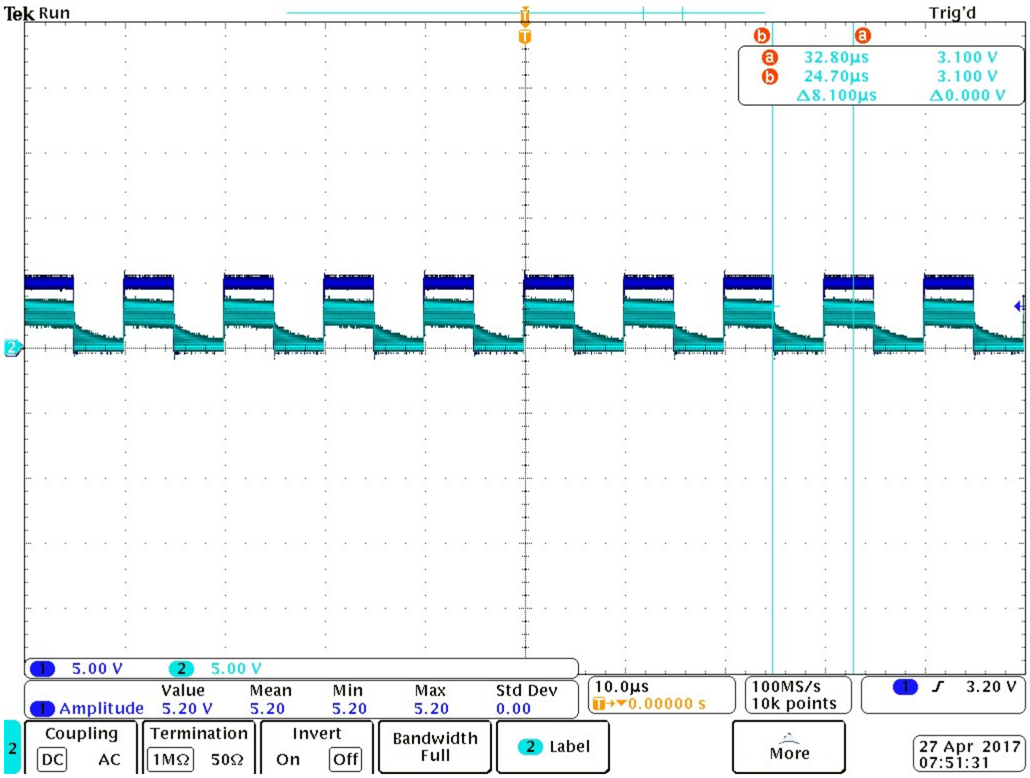


Figure 79 - Tested PCA9306 level shifter with 3.3V Square Wave

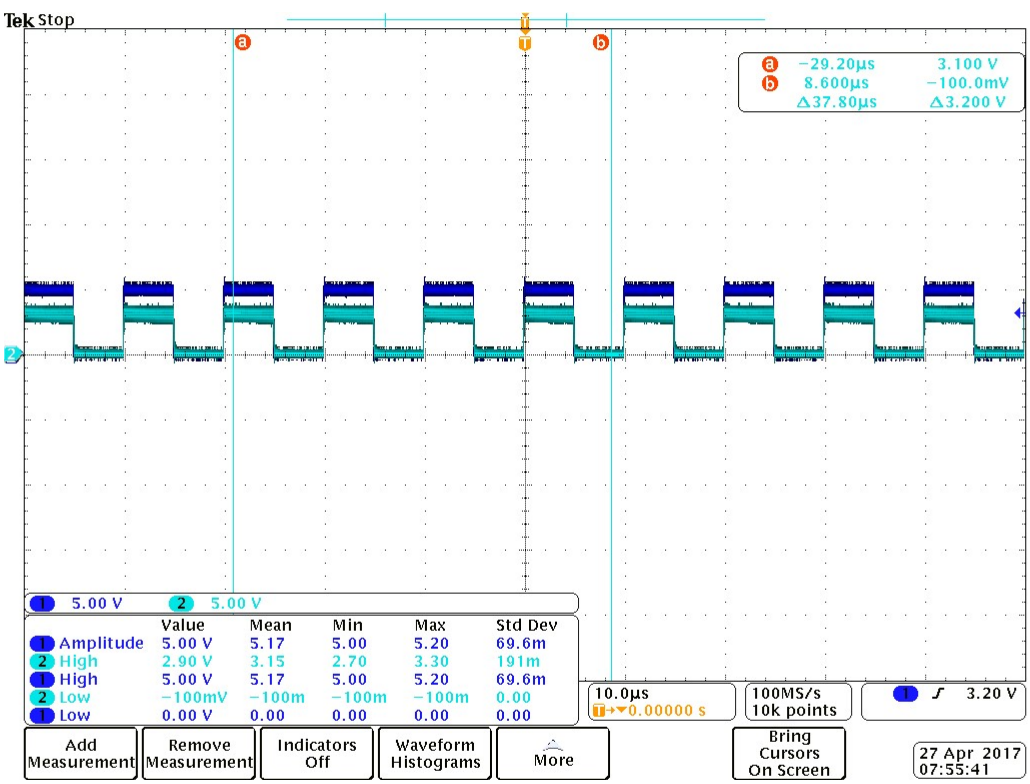


Figure 80 - Tested PCA9306 level shifter with 5V Square Wave

6.0 Build Phase Revisions

During the construction of the project several changes were made to accommodate unforeseen complications. In this chapter we will go over each of the changes that were made and the problems that remedied by those changes.
PCB Related Modifications:

6.1 PCB Related Modifications

This section will cover all the parts and circuit design changes that were made that affected the PCB.

6.1.1 Removal of Op-Amp Circuit

With the testing of a new, slightly larger electret microphone, our preamp circuit gave the output a 2V range, which was more than enough to use with the atmega328, which allowed us to remove the op-amp circuit, and subsequently reduce the footprint of that circuit drastically. This allowed us to remove noise, added physical instrumentation, and allowed us to fine-tune the sensitivity with code.

6.1.2 Removal of Primary Board level shifter

The fingerprint module was able to accept 5V logic levels, which allowed us to remove the logic level shifter on the main board shifter.

6.1.3 Removal of 3.3V regulator

With the removal of the need for the main board logic level shifter, we were able to utilize the beaglebone's own reference for the beaglebones level shift, allowing us to remove all references to the 3.3V regulation.

6.1.4 Solenoid MOSFET Modification

In the initial testing, we used a BSS138 MOSFET to actuate the solenoid but we since the solenoid had a draw of 330 mA that it was operating outside the specified range of BSS138 which was only a 200mA current. With this problem, we researched a other MOSFETs with higher operating current and ended up purchasing the Fairchild 512-NDS355AN which is a surface mount MOSFET with the same footprint as the BSS138 which kept the pcb from having any drastic alterations. The new MOSFET works with the same gate voltage but has a maximum drain current of 1.7A which is better suited to for the solenoid.

6.1.5 USB Charging Circuit

The LT8608 was near end-of-life so we decided to go with TI's TPS2514, which proved to be quite effective, as we could use the already existing regulator to charge the phones, and simply have the IC take care of the appropriate voltage levels on the D+ and D- pins. There were a couple of alternatives, such as following some of the basic standards, such as the Dedicated Charging Port section of the USB BC 1.2 standard. The current was limited by the Regulator IC. This proved to be the most power efficient layout, without creating too large of a footprint. The USB charging circuit was placed on a different PCB for the Demo, to account for last minute time constraints, but there was plenty of room on the main PCB, with the removal of the op-amp circuit, to add the charging circuit given the opportunity for a final implementation.

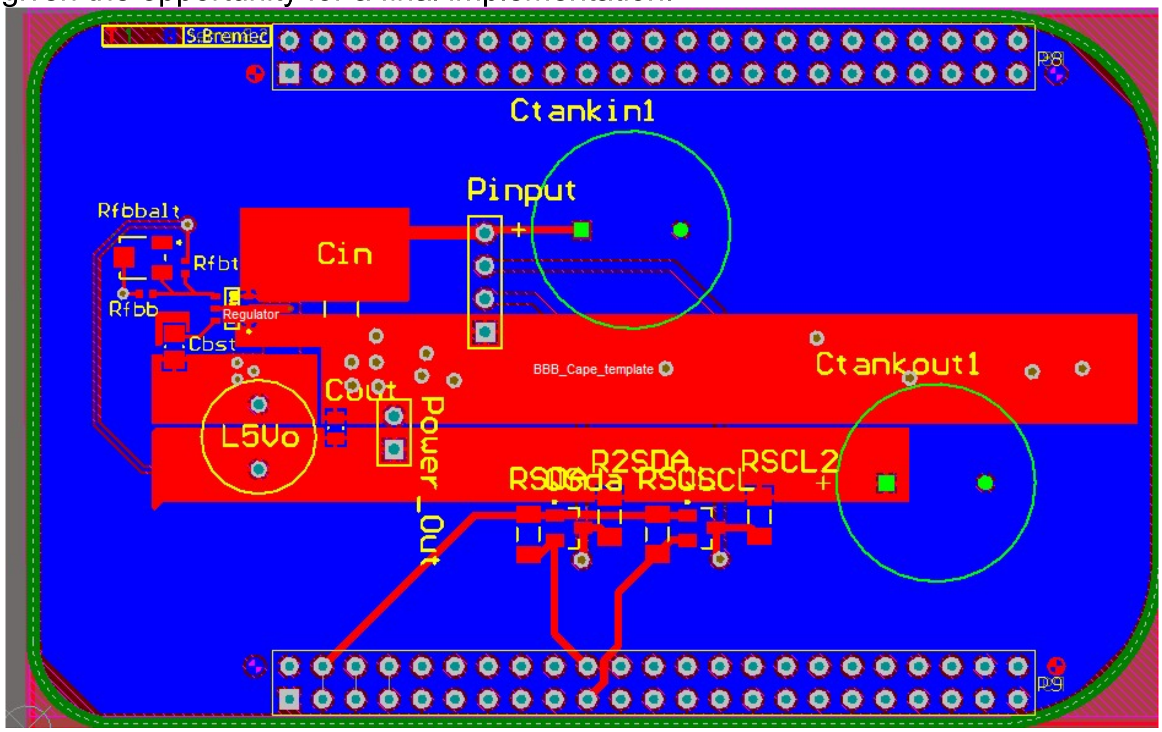


Figure 81 - USB Charging Circuit PCB

6.1.6 Final PCB Layouts

The following images show the final layout of the PCB. Figure 82 shows the top layer of the PCB that handled the security and the sensors. Figure 83 shows the bottom side.

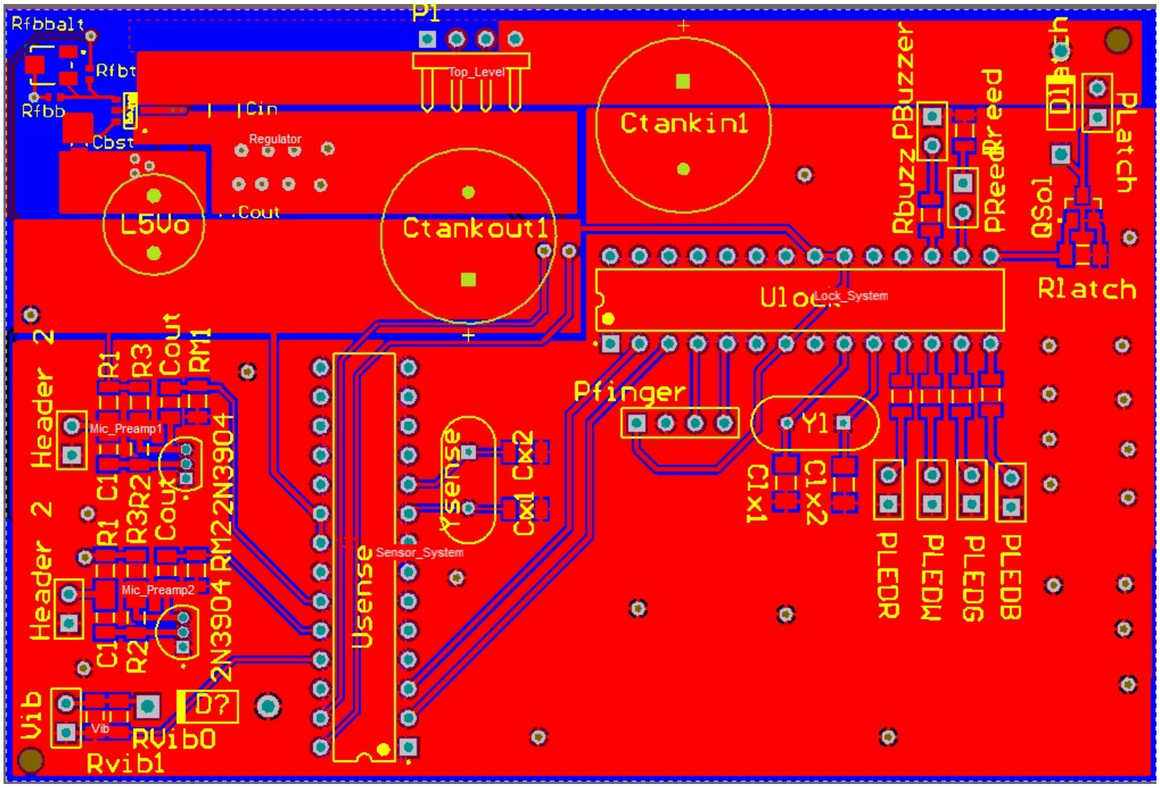


Figure 82 - Top Layer of Final PCB

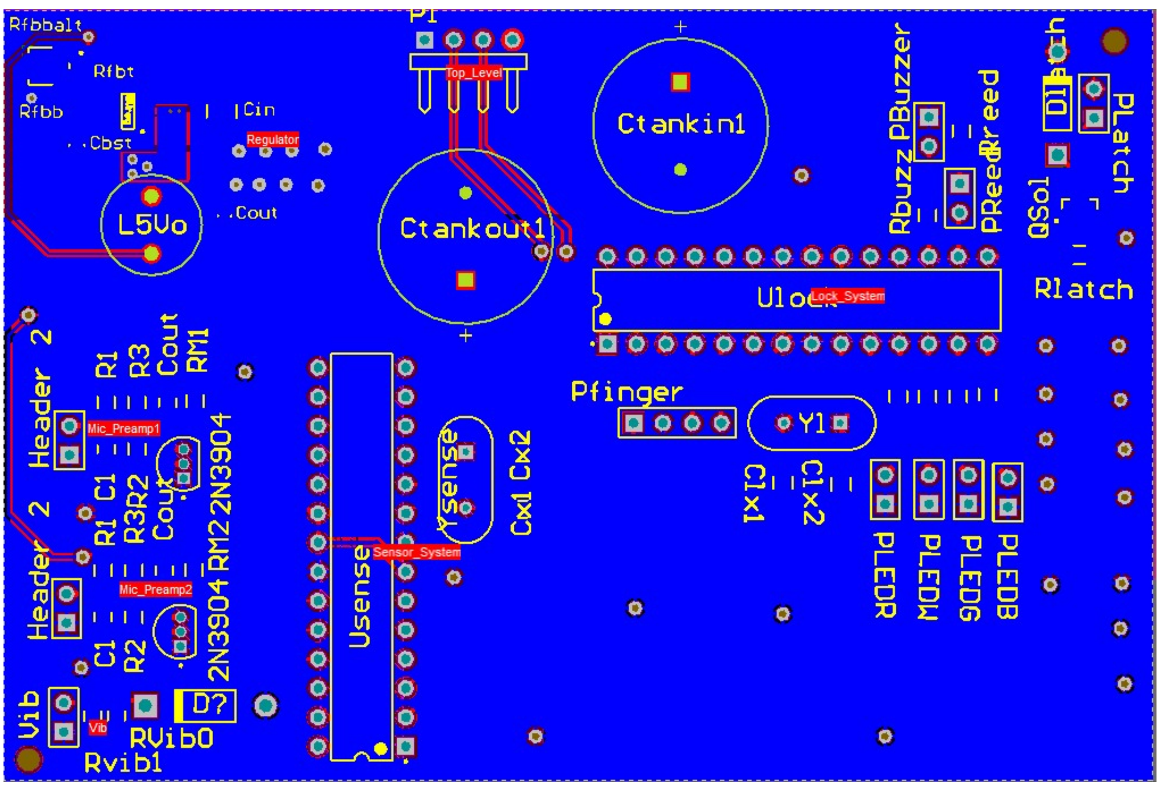


Figure 83 - Bottom Layer of Final PCB

6.2 Finalized Process Flow

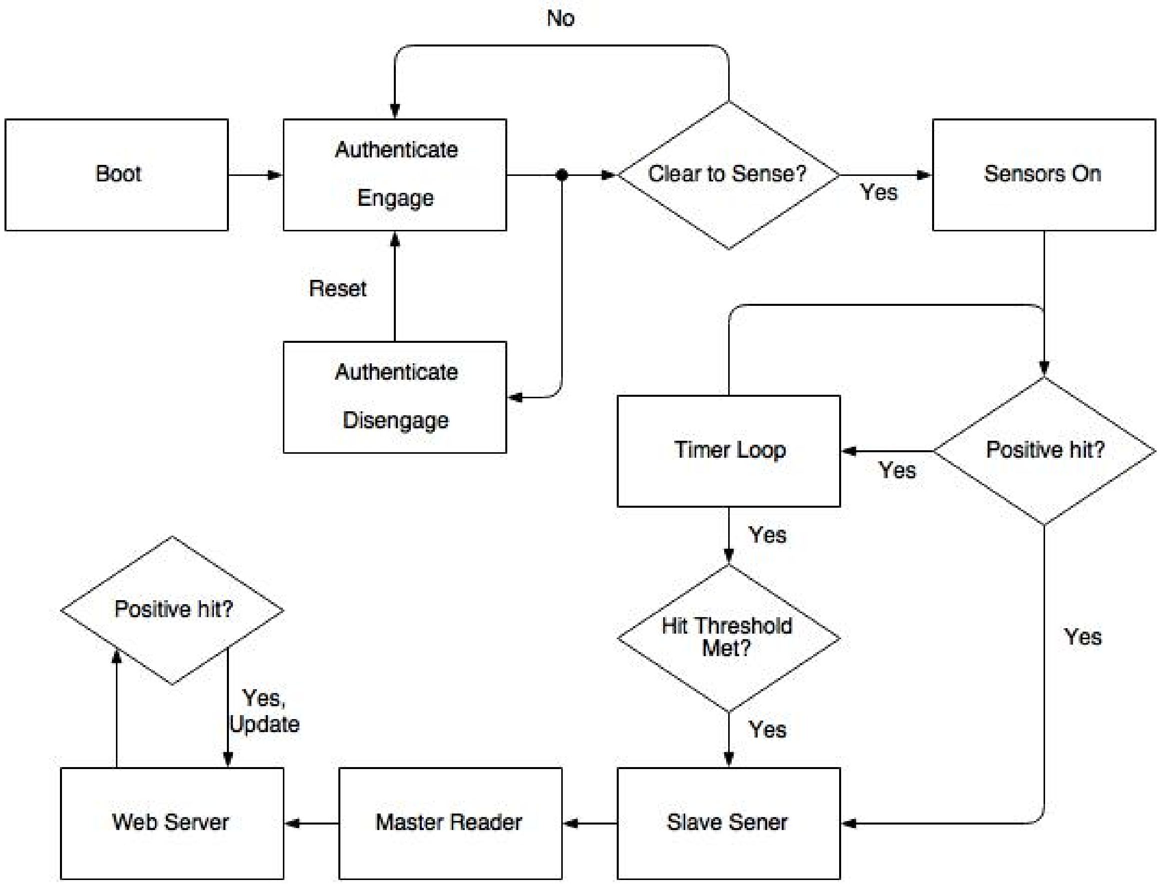


Figure 84 - Final Process Flow

When the device boots, it undergoes a boot sequence in which the device starts to initialize the different chips on the PCB. The programming will tell the hardware to play a sound sequence and initialize the diagnostic LED display upon being powered by the 120v wall outlet. After the sound and LED's are initialized, the chip containing the code for the fingerprint module will begin to initialize the fingerprint module. Once the fingerprint module is initialized, the device is ready to be used. During this time, the fingerprint module is sending a signal to the sensor unit to not begin sensing until a fingerprint has been authenticated. To authenticate a fingerprint, the user must put their finger on the sensor. Upon doing this, the system stores an image of the print and then requires the user to rescan their print in order for the system to match the rescan to the first print. When the match is confirmed positive, the fingerprint module throws a flag to the sensor unit to turn the sensors on and prime them to sense.
After the user places their cellular device in the box, the sensors will continue to monitor them until the sensor unit gets hit with another flag to stop sensing (when the user pulls their device from the box when they finish using it). The system will run cycles of samples looking for the sensors to pick up signals. If a certain number of samples in a single cycle read an appropriate amount of input, the

system will throw a flag stating that the box has detected a positive hit for a ping on the cellular device. The system only needs to detect vibration of a certain magnitude for the sample to be considered a hit. For the system to consider a sound to be a positive hit, it has to take both inputs from both microphones and compare them. If both values seen across both microphones are comparable in magnitude, the system will consider the sample a positive hit for the cycle. Vibrations are thoroughly isolated via the structure of the system, but sound can still bleed through. This comparison reduces the chance of bleed through causing false positives to be thrown across multiple boxes. The first time the box throws a flag for a positive hit, the system will then throw a timer to start counting the number of times the cellular device in the box is pinged during the extent of that timer. If the cellular device is pinged a certain number of times during this timer period, the device will throw another flag denoting that there might be a possible emergency because the device is being pinged a lot in a short amount of time as would normally be done in an emergency situation.

During all of this, the device is continually passing these flags to the slave sender. The slave senders will each designate their own address on the I2C bus. The master reader will keep cycling through each of the devices on its own I2C bus, pulling whatever status flag the slave sender is currently holding that it received from the sensing circuit. The master reader will then pass these flag values to a bash script stored on the Beaglebone Black. The bash script will take these values and appropriately update the external web page for each new value it reads. When the user is done using the box, they will simply place their print on the scanner once more. The scanner will send a signal to the sensor module to turn the sensors off, and when the user opens the box to get their cellular device, a flag will be thrown for the master reader to clear the values on the webpage for that box. The system will now be available to be used by the next user.

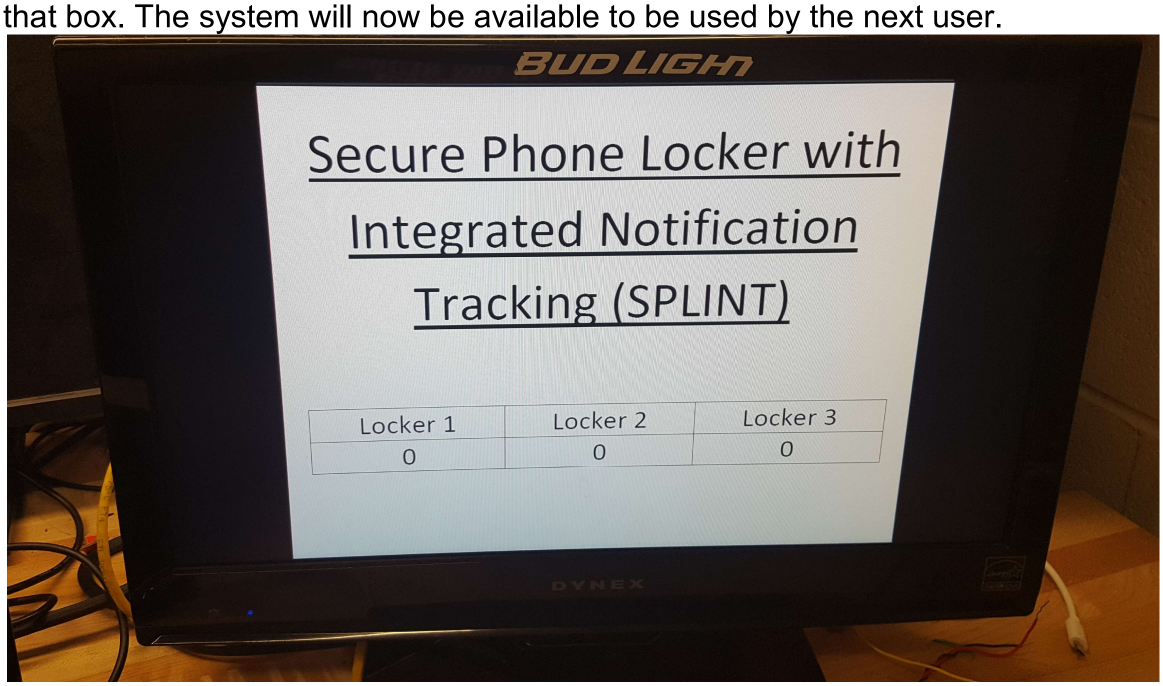


Figure 85 - FInal Web Page Display

6.3 Standards and Constraints

In this section we will discuss all of the related standards and constraints that either apply to or affect our project. We will give a brief overview the constraint or standard and will elaborate on how we will address each issue that affects us.

6.4 Requirement Specifications

Below we will discuss the marketing requirements and the engineering requirements that we will design our system around.

6.4.1 Marketing Requirements

1) The system will be low cost to make our product reasonably affordable for the consumer market.
2) The sensors in our to device should be reliable and long lasting.
3) O system to be small enough to be conveniently installed without being an obstruction to existing spaces.
4) Our system should be power efficient enough to be comparable with existing charging accessories.
5) Our system will have necessary security features in place to keep each phone secure.

6.4.2 Engineering Requirements

1) The device should be fully powered by a standard 120V 15A wall receptacle.
2) Our microphone sensors should have a minimum sensory threshold that is no greater than 80 dB.
3) Our vibration sensors should be able to detect vibration frequencies between 1 kHz and 2 kHz. (1-2 kHz is the operational vibration frequency range found it the majority of phone vibration motors.)
4) Our individual holding compartments should have no less than an 80% damping of vibration and noise between compartments.
5) Our systems container footprint should be no more 12”x12”x36” and able to hold a minimum of three phones.
6) Our system should consume no more than 400 Watts of power with all 3 phones charging.
7) Our locking system should require fingerprint authentication with accuracy >90%
8) Device should have less than a 5 second delay between sensor actuation and transmission of notification
9) There should be an emergency override in case of power loss that allows for users to reclaim their property.

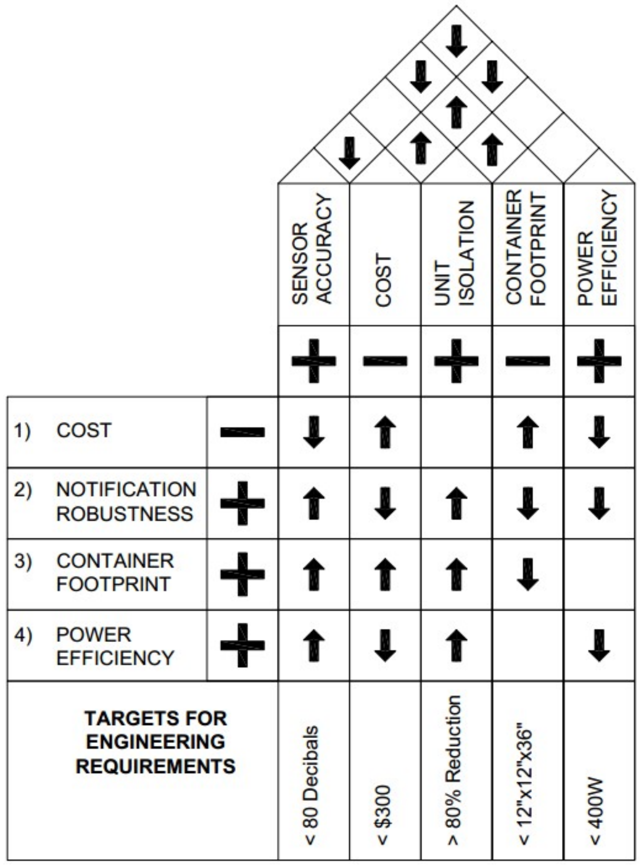


Figure 86 - House of Quality

6.5 House of Quality

Taking into consideration the robustness of the design versus the requirements needed to facilitate said capacity, we will need to optimize the design to consider the design priorities, with respect to trade off consequences. The house of quality will assist as a visual aid and reminder to consider the cost of components while narrowing down the specifications of the design.

One of the largest design considerations when making this will be distinguishing the compartments with the sensors, while accurately being able to detect notifications. Convenience is a major priority in the design, which also makes unit isolation and sensor accuracy a priority.

The less accurate the sensors are, the less of a convenience it becomes and the more of a hassle it will be. Similarly, if the containers are too large, it would be inconvenient to use or implement the design. Power efficiency and price do not directly impact convenience, which gives the design a few degrees of freedom.

In this graph security includes privacy, and more security will mean more components which means more cost, and the more components we add to the compartment, the more space it takes up. So it will be ideal to find a solution that encompasses an accurate reading of notifications with the least components, while preventing false readings and being as accurate as much as possible.

6.6 Standards

Standards are pre-existing rules, limits or definitions that act as minimum acceptable benchmarks which are typically put forth by a government agency, professionals or another entity. There are legal standards such as laws, and statutes which are enforced by the government, as well as ethical standards which are based in trust, fairness, and professional courtesy which aren't as clean cut as laws. There are also standards that arise out of necessity for things to be able to work together such as USB standards which requires USB ports to always have the same pin-out as well as a bare minimum for performance which many other products rely on to be able to function properly. Below we will discuss the major standards that will be affecting our project and design.

6.6.1 USB Standard

This section will cover the relevant Universal Serial Bus (USB) standards that which must be taken into account in if project design. Below in Figure 87 you will see Type A (most common) on left, and type B (not as common) on right.

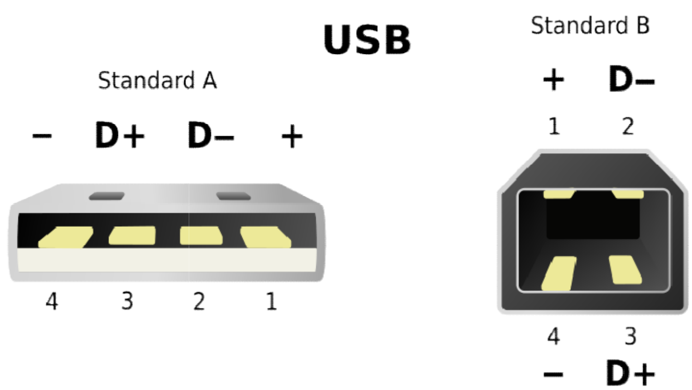


Figure 87 - Pinout for USB heads

6.6.1.1 USB specifications

USB has a variety of specifications and requirements for different categories of power. [1] [2] For a simple phone charging station, this project will fall under the battery charging specification. [3]

All dedicated charging ports fall under Charging Ports (section 4.1 of the Battery Charging Specification, Revision 1.2) The specifications found that generally apply to all charging ports are:

- The D+ and D- need to be shorted
- The output voltage overshoot cannot exceed 6V
- The output current cannot exceed 5A at any point

- If the current drawn by a portable device (The phone) causes this port to go out of operating range, then the port is allowed to shut down. This can be achieved through turning off the power bus, constant current limiting, or foldback current limiting.

- The output charging voltage of a charging port shall remain within -0.3V and 9V for any single point failure in the charging port.

- If a device has multiple charging ports, each charging port shall stay within its required operating parameters, regardless of the operation of other charging ports. Below in Figure 88, we see an example of different operationg curves from battery charging specification Revision 1.2, section 4.4.1. (Reprinted with permission from USB.org[23])

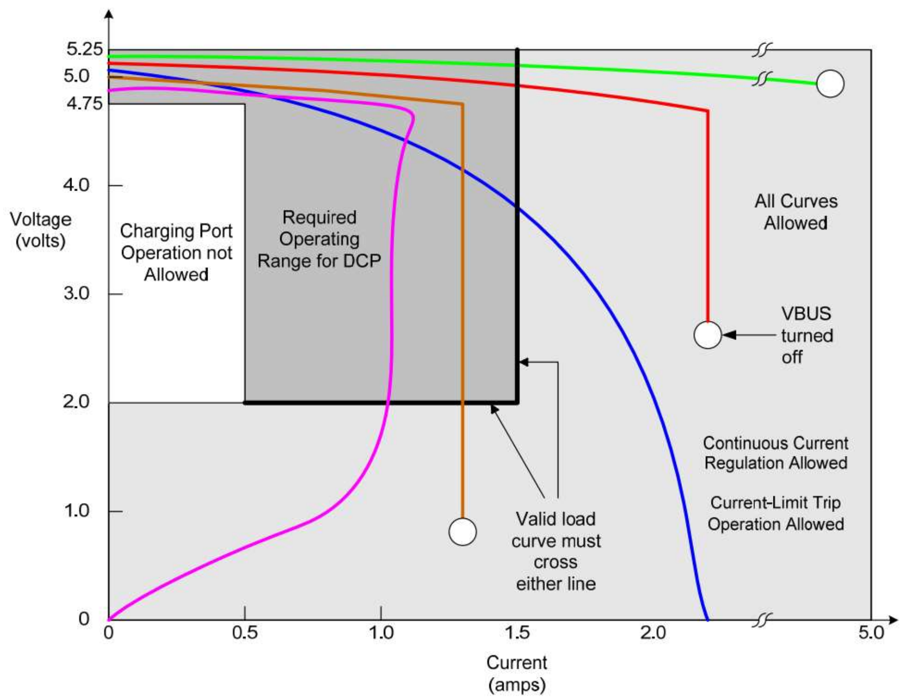


Figure 88 - Example operating curves from Battery Charging Specification

Our particular device falls under the Dedicated Charging Port (DCP) category Shutdown conditions which includes:

- A DCP shall output a voltage between 4.75 and 5.25V for any current less than 1.5A

- The voltage on VBUS is averaged over a time of 250ms

- A DCP shall not shut down if the load current is less than 1.5A and the load voltage is greater than 2.0V

- A DCP is allowed to shut down for load currents greater than 1.5A, or for load voltages less than 2.0V

- Once this occurs, the general shutdown methods apply
- A DCP is NOT ALLOWED to shutdown within the operating conditions.
- Figure 4.2 (From the specification sheet see appendix 7.2.1) shows an several example curve
- When the load current shifts from Idcp_low(I<=30mA) to Idcp_mid(30mA<=I<=100mA) or from Idcp_mid to Idcp_hi (I>=100mA) the voltage shall drop to no lower than 4.1V
- This is a only a requirement for Idcp_mid to Idcp_hi transitions that occur 20ms after the transition from Idcp_low to Idcp_mid
- The undershoot shouldn't last longer than 10ms
- For transitions from Idcp_low to Idcp_hi, the output voltage of the dedicated charging port can drop to the load voltage of the attached device for 10ms
- After this timeframe, it should continue on with normal operating parameters.
- *Data Pin short*
- The D+ and D- pins should have no more than 200ohms ohms between them
- The leakage current should be less than 6A

The actual port of the Dedicated charging port, for our purposes, should also e a Standard-A Receptacle. The information for this standard can be found under Appendix A.1 USB 3 Cable & Connector Compliance document. [found at 4]

6.6.2 Security Standards

Security is a massive industry with many laws and standards in place to protect people's privacy and personnel data. When designing our project we need to ensure that we comply with these laws that are currently in place as well as minimize areas of concern.

6.6.2.1 Biometric laws and concerns

Biometric authentication poses a unique concern that no other form of identification has to deal with; they are absolute, unique identifiers that cannot be replaced. Extra care must be taken when storing biometric data because increasingly more often, they are being used to access finances or other sensitive information and can have a lasting impact if the data is compromised. If a social security number becomes compromised, it can be whereas if biometrics, being biologically unique to a particular individual, cannot be replaced. This would leave the individual at heightened risk for identity theft, where the only option would be to withdraw entirely from biometric-facilitated transactions[24].

There are several laws that have popped up associated with the use of biometric data and its security and handling in recent years in different states[25] but they all have similar wording such as the following from the Biometrics Information Privacy Act 740 ILCS 14 section 10:

> "A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines"[26]

Within our project we will have multiple fingerprint scanners that will be collecting biometric data on individuals that we will need to ensure is protected. This data will be collected from the fingerprint sensor and will be stored locally within the fingerprint sensor circuit, giving a strong layer of security for the data through isolation. This will be our primary means of data protection for the biometric data and the secondary protection will be the housing itself which will not have the circuitry accessible to physical tampering.

6.6.3 Sensor Standards

There has been a rising usage of sensors in the world, notably from the new surge of activity with the internet of things, consumers are more than ever using sensors from everyday home projects to new applications for it in the work environment. With IOT, sensors are now readily available for many people of various expertise levels to use. Due to this activity IEEE has set new standards specifically for sensors that specify performance, units, conditions, and limits. These parameters are to facilitate distribution and implementation of sensors since there are several different types of sensors, manufacturers, vendors and software that use it. In this way the consumer will have a component that has an acceptable performance level while at the same time having the flexibility for product differentiation and innovation. Some of the sensors that they've specified are accelerometers, magnetometers, gyrommeter/ gyroscope, baramoter/ pressure sensors, hygrometer/humidity sensors, temperature sensors, ambient light sensors (ALSs) and proximity sensors. In this project, standards on accelerometers, pressure and position sensors are the only ones that apply for our application.

6.6.3.1 Accelerometer Standards

As defined an accelerometer is a "A sensor that measures the rate of change of velocity (i.e., acceleration), typically in the International System of Units (SI) form of meters per s squared (m/s2) or g1". In our case the accelerometer is measuring low to high frequencies, and producing a constant variable voltage based on the amount of acceleration applied to the accelerometer. An accelerometers accuracy is extremely important and so it is essential to fully understand the primary contributors to absolute acceleration error. The following only applies to digital accelerometers but they are: the Full Scale Range (FSR), digital bit depth, zero-g offset, sensitivity, noise, current consumption, ODR, the 3dB cutoff of a filter, internal oscillator tolerance, cross-acris sensitivity, integral non-linearity, transition time and data ready relay. All of these need to be specific thoroughly so that there are no accuracy errors.
The below table will show in detail the standards that we most need to take into consideration in our project.

Table 26 - Acceleration Sensor Standard Specifications

Parameters	**Definition**	**Unit of measure**	**Condition**	**Distribution**
Full Scale Range	Peak–to-peak measurement range of the sensor per each orthogonal axis.	g (9.81 m/s2)	At room temperature (25 °C), At operating voltage, At final test, After PCB assembly (place and reflow), Over life, After mechanical shock, For each selectable mode.	Minimum: –3 sigma limit Typical: ± (Target FSR (g)) / 2 Maximum: +3 sigma limit
Sensitivity	The change in acceleration input corresponding to 1 LSB change in output.	g/least significant bit (LSB)	Specified for each orthogonal sensing axis, Specified for each selectable FSR, At RT (25 °C), At operating voltage, After PCB assembly (place and reflow), Over life, After mechanical shock	Minimum: –3 sigma limit Typical: Mean Maximum: +3 sigma limit
Noise	The smallest measurable change in acceleration expressed as rms and calculated as the standard deviation of a minimum 10 000 sample points under vibration isolation.	mg (rms)	Specified for each orthogonal sensing axis, Specified for each selectable ODR/filter combination, Specified for each selectable FSR, At RT (25 °C), At operating voltage	Minimum: –3 sigma limit Typical: Mean rms Noise Maximum: +3 sigma limit
Current Consumption	Measured current consumption.	μA (micro-ampere)	–40 °C to 85 °C, For operating voltage range, Specified for each selectable power mode, Specified for each ODR	Minimum: –3 sigma limit Typical: Mean Idd Maximum: +3 sigma limit

As seen above, the range of the accelerometer is important for us. In our application, it needs to pick up vibrations so the range needs to be wide enough to pick up cell phone vibrations. The sensitivity specified is so that the sensor can detect that there has been an acceleration surrounding it so that it can then output a voltage. Noise is very important as it can distort the signal and cause the function to not work correctly, either sending a signal when there is vibration or when it does not. Lastly the current consumption on our device will be under those temperature restraints and making sure that there is an appropriate amount of current flowing to the accelerometer so that it works properly.

6.6.3.2 Pressure Sensor Standards

As defined a pressure sensor is a “A sensor that measures atmospheric pressure, typically in the SI unit form of hecto-Pascal (1 hPa = 100 Pa = 1 millibar)”. In our case the pressure sensor is acting as a transducer, which senses the pressure as it converts it to an electrical signal. A pressure sensors relative accuracy is extremely important as the altitude reference in a fused location system and so it is essential to fully understand the primary contributors to absolute pressure error. The following only applies to digital sensors but they are: the Full Scale Range (FSR), digital bit depth, pressure temperature coefficient, pressure accuracy, sensitivity, noise, current consumption, integral non-linearity, acquisition time, transition time, short term stability(STS), long term stability(LTS) and over pressure maximum. All of these need to be specific thoroughly so that there are no pressure errors.
The below table will show in detail the standards that we most need to take into consideration in our project.

Table 27 - Pressure Sensor Standard Specifications

Parameters	Definition	Unit of measure	Condition	Distribution
Full Scale Range	Peak-to-peak measurement range of the sensor	hPa	Specified for each selectable mode, At RT (25 °C), At operating voltage, At final test, After PCB assembly (place and reflow), Over life, After mechanical shock	Mean and standard deviation of minimum. Mean and standard deviation of maximum.
Pressure Accuracy	Pressure measurement accuracy over the entire measurement range	hPa	Over FSR, At RT (25 °C), At operating voltage, After PCB assembly (place and reflow)	Minimum: –3 sigma limit Typical: Mean Maximum: +3 sigma limit
Sensitivity	The change in pressure input corresponding to 1 LSB change in output.	hPa/LSB	At RT (25 °C), At operating voltage, For 700 hPa to 1100 hPa range, After PCB assembly (place and reflow), Over life	Minimum: –3 sigma limit Typical: Computed target (LSB range / FSR) Maximum: +3 sigma limit
Current Consumption	Measured current consumption.	µA	Specified for each selectable power mode, Specified for each selectable ODR, –40 °C to 85 °C, For operating voltage range	Minimum: –3 sigma limit Typical: Mean Maximum: +3 sigma limit

As seen above, the range of the pressure sensor is important for us. In our application, it needs to be able to detect when there is a phone in the hub and if it starts vibrating. The range is important, the phone will be sitting on top of the sensor and if it can only be mounted on the wall then it won't be able to pick up the vibration as easily. The accuracy is also of significance, the sensor needs to be able to send the correct information or it may miss a notification. The sensitivity is significant in more than one way. If it is too high then it won't be able to tell the phone is vibrating, and if it is too low then it will detect outside noise as a real signal, which leads into the noise. Noise will distort the signal and significantly affect the data. We will be taking precautions to minimize the effects of noise. Also current consumption is important, if it doesn't receive the correct current then the sensor won't work at all times.

6.6.3.3 Position Sensors

As defined a position sensor is a "A sensor that measures object locality in the distance unit form of cm". In our case the position sensor is detecting when opposite magnets have come together, which then changes the current from changing between a normally open circuit or a normally closed circuit, or vice versa. If they have no distance apart, then the magnets have come together and thus it changes the state from normally open to normally closed. A position sensors accuracy is extremely important and so it is essential to fully understand the primary contributors to absolute position error. The following only applies to digital sensors but they are: Digital bit depth, sensitivity, sensing current consumption and transition time. All of these need to be specific thoroughly so that there are no measurement errors.

The below table will show in detail the standards that we most need to take into consideration in our project.

Table 28 - Measurement Sensor Standard Specifications

Parameters	Definition	Unit of measure	Condition	Distribution
Sensitivity	This is applicable to proximity modules that leverage integrated LEDs. Curves showing the proximity sensor's detection sensitivity over its FSR represented by a minimum, typical, and maximum distribution (see Figure 10).	LSB	Specified for range of reflective material properties, Specified for range of IR LED drive current/pulses, At vendor's recommended ADC conversion time, At RT (25 °C), At operating voltage	Minimum: –3 sigma limit Typical: Mean Maximum: +3 sigma limit
Sensing current consumption	Measured current consumption.	μA	Specified for all selectable operating modes, –40 °C to 85 °C, For operating voltage range	Minimum: –3 sigma limit Typical: Mean Idd Maximum: +3 sigma limit
Transition Time	Measured transition time between two specified states as illustrated in Figure 2. It is expected that some of these parameters may only be validated through design simulation. See Clause 3 and 4.1 for state definitions.	ms	Specified for power on to ready/active state (Ton), Specified for inactive to active state (Tmr1), Specified for operational mode changes (Res, FSR) (Top), At RT (25 °C), At operating voltage	Minimum: –3 sigma limit Typical: Mean Maximum: +3 sigma limit

As seen above, the range of the position sensor is extremely important for us. It will only close once the magnet is close enough to each other that the poles will switch, creating an opposite and attractive charge and thus close the circuit. The sensitivity will affect whether or not the magnet will be able to affect the reed sensor so that it changes the state of the circuit. The reed sensor will have a necessary voltage to operate and so the current consumption will come into effect. The sensor will be on at all times for whenever someone needs to open or close the door of the devices to place or retrieve their phones. Lastly the transition time is significant since that sensor will be continuously changing states maybe multiple times a day.

6.6.4 *Other Regulations*

When doing our research, we looked into various agencies and laws that we thought might have some applicable rules that we would need to abide by. Upon further research, aside from the previously stated standards and constraints, we could find no applicable regulations or policies that applied to the use or construction of our project from the following:

- Consumer Product Safety Commission (CSPC)
- Americans with Disabilities Act of 1990 (ADA)
- Environmental Protection Agency (EPA)
- Occupational Safety and Health Administration (OSHA)
- National Fire Protection Association (NFPA)

It should be noted that while the NFPA has rules and regulations in place regarding Stationary Storage Battery Systems in NFPA 1 Chapter 52 [27] which cover safety venting, spill control, neutralization, and air flow ventilation, these rules all have exceptions for lithium-ion and lithium-ion metal polymer batteries which is the type that is used in all modern phones that our chambers would support for charging.

6.7 Constraints

Constraints are any physical restrictions or real world limitations that we face in our design process. The majority of constraints are largely self-imposed by the marketing and engineering requirement specifications that we have agreed to work towards for a quality project. Some constraints however, are nearly uncontrollable, such as the limitations of knowledge. Fortunately for us, there are very few uncontrollable constraints which are pretty much limited in our design process to sheer bad luck which we can deal with by allowing ourselves enough time for corrections. Below we will cover the constraints we have that will affect our design.

6.7.1 Phone Chamber Dimension Constraints

There are several physical dimensions to take into account when designing the size of the phone chamber. To keep our chambers reasonable we will constrain ourselves to only be looking at phones that are not considered to "phablets" which are by definition oversized to the point that they are nearly small tablets. The largest phone we will be considering will be a Galaxy Note 5 which has dimensions of 6.03" x 3.00" x 0.30." A major inhibiting factor in this design is what we choose to insulate the walls with to dampen the noise between chambers. This will need to be prototyped and measured to get an exact thickness for the walls between chambers. We also need to provide room for the various sensors as well as the locking mechanism and the controller. We may be able to reduce the sensitivity of the sound sensor to compensate for bleed through sound which may allow us to reduce the amount of insulation required.

7.0 Administrative

Under this administrative section we will discuss the decision making process and management structure we used when collaborating, researching and designing this project. This will cover the projects budget, financing and funding as well as our milestones. It will also cover any administrative conflicts we encounter and the steps we took to resolve them.

7.1 Project Management

The management of this project was mostly a team effort that required input from all members in the decision making process as well as the budget and financing.

7.1.1 Project budget and Financing

Our list of major expenses is shown below in Table 29.

Table 29 - Project Expenses

ITEM	Manufacturer	QUANTITY	COST
Microcontrollers			
Communication Controller	BeagleBone Black	1	$62
Chamber Controller	ATmega328	6	$30.00
Printed Circuit Boards			
Various Boards	Design printed by Elecro	12	$10.00
Sensors			
Vibration Sensors	MINI SENSE HORIZ MNT VIBRATION	5	$25.50
Microphones	Goedrum Prewired 35mm Piezo Disc	5	$11.90
Major Components			
Fingerprint Scanner	K202 control board w R303 fingerprint scanner	3pc	$100.00
Solenoid Lock	FCBB High Quality 6 Holes Dc 12V	4pc	$27.36
Miscellaneous Components			$30.00
Locker Materials	Varies		$30.00
Main Construction Material	TBD		$20.00
Sound Insulating Material			$10.00
Miscellaneous Hardware			$10.00
TOTAL			$214.82

The project is currently self-financed by the group members, where each member will contribute an even amount of funds. However we are still trying to find a sponsor, so the budget may change based on that. Microcontrollers are pretty affordable whether we use TI products or an Arduino. PCBs are also estimated at a low cost based on how the individual components are cheap by themselves. We are going to have three charging stations and each one will be built with materials so as to be vibration resistant to not interfere with the sensors picking up the signals from the phone. We also intend to have heat resistance materials to keep the phones cooler while charging. We have sensors in mind that we'd like to use and those are the prices found online for each sensor. The price for the power unit is a rough estimate and the LEDs are estimated based on LED's found online that will provide a decorative feature and an indication light that we need for the user. These are the basic materials that we know we will need and an idea of how much they will cost, however this may change once we start testing and building the final product.

7.2 Initial Project Milestone: Senior Design I - Spring 2017

There are a few things we would like to accomplish for the first semester. The first thing we need to do is brainstorm ideas, collaborate and narrow down which projects would best utilize our individual strengths and select our project. Second, Once our project is selected, we will research methods, specifications and standards as well as any similar products to determine how best to go about implementing our idea. Third we will conceptualize our idea and collectively decide which major systems we will need and who will work on each part. After the work load is distributed, we will individually research and figure out what components are needed for each system within the project and then research and determine specific components we will use by comparing different products based on availability, capability, functionality, compatibility, and price.

By the end of Senior Design 1, in addition to the completed research paper, we intend to have a series of design schematics that can be shown to work on paper as well as have an initial test board that we can run functionality and proof of concept tests on before we actually start fabricating a final board in the second semester. Below in Table 29, we have created a schedule of major milestones. It shows the outlook through senior design 2.

Table 30 - Project Schedule

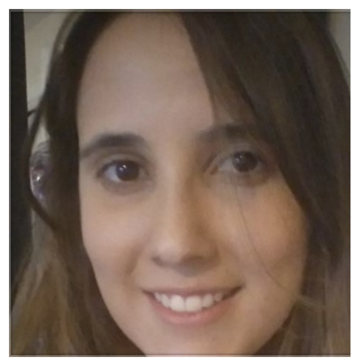
Milestone	Task	Start Date	End Date	Status
SENIOR DESIGN 1				
ADMINISTRATIVE OUTLOOK				
A	Project Selection	1/17/2017	1/31/2017	Complete
B	Assign Responsibilities	2/1/2017	02/08/17	Complete
C	Initial Project Document	1/31/2017	2/3/2017	Complete
D	Table of Contents	2/7/2017	3/24/2017	Complete
E	Draft Document	2/7/2017	3/29/2017	Complete
F	Final Draft	4/1/2017	4/25/2017	Complete
TECHNICAL OUTLOOK				
1	Component Research	2/1/2017	4/14/2017	Complete
2	Component Gathering	2/1/2017	11/27/2017	Complete
3	Component Testing	3/30/2017	11/28/2017	Complete
4	Circuit Design	3/24/2017	4/25/2017	Complete
5	Circuit Testing	3/30/2017	11/30/2017	Complete
6	User Interface Design	3/30/2017	11/30/2017	Complete
SENIOR DESIGN 2				
ADMINISTRATIVE OUTLOOK				
G	Critical Design Review	-	9/22/2017	Complete
I	Conference Paper	-	11/17/2017	Complete
J	Mid-Term Demonstration	-	10/30/2017	Complete
K	Final Presentation	-	11/29/2017	Complete
TECHNICAL OUTLOOK				
7	User Interface Design	-	11/30/2017	Complete
8	PCB Design	-	11/15/2017	Complete
9	PCB Implementation	-	11/29/2017	Complete
10	Final Product	-	12/1/2017	Complete

7.3 The Team

Ian Flemings is currently a senior at the University of Central Florida and will receive Bachelor's of Science in Electrical Engineering. He has held a engineering internship position with AECOM for the last 2 years and in that time he has taken and passed the Fundamentals of Engineering exam for electrical and computer engineering, and has accepted a job with Power Design as an Associate Designer in their Electrical Engineering department

Nicholas Lucas is currently a senior in Electrical Engineering at UCF with a minor in mathematics. He passed the fundamentals of engineering exam and his E.I. status is pending graduation. He wishes to go into the industry in either RF, networking or distributed computing, and plans to continue to pursue a masters in Electrical Engineering or Computer Science.

Alexander Masterson is currently a senior at the University of Central Florida. He is currently seeking a Double Major with a Bachelors degree in Computer Engineering and a Bachelors in Electrical Engineering. He will graduate in December of 2017. He is pursuing a career in system automation controls. He is currently seeking full time employment for when he graduates. He plans to work in the field for a while and then may pursue a Masters Degree in the future



Evelin Santana is currently a senior at the University of Central Florida. She is currently completing a Bachelors degree in Electrical Engineering and wants to graduate in December of 2017. She is currently seeking to accept a position for Controls Systems Engineer with the Disney Imagineering Team when she graduates.

8.0 Appendices

This section consists of various appendices which will detail our references, provide any necessary additional documentation, show applicable copyright permission usage requests, as well as an index of various items that may be referenced multiple times within the document.

8.1 Works Cited

[1] Lazar Rozenblat, "SWITCH MODE POWER SUPPLY TUTORIAL," [Online]. Available: http://www.smps.us/power-supply.html.

[2] Wikipedia, "Fingerprint Recognition," [Online]. Available: https://en.wikipedia.org/wiki/Fingerprint_recognition.

[3] J. R. A. M. Ralph A. Sittnick, "Electromagnetic door lock system". US Patent 4763937, 11 Sep 1986.

[4] "Linear Solenoid Actuator Theory and Tutorial," ElectronicsTutorials, [Online]. Available: http://www.electronics-tutorials.ws/io/io_6.html. [Accessed 28 3 2017].

[5] TLX Technologies, "Latching Solenoid Theory," [Online]. Available: http://www.tlxtech.com/understanding-solenoids/theory-operation/latching-solenoid-theory. [Accessed 23 March 2017].

[6] "ISO/IEC 7810:2003," International Organization for Standardization, [Online]. Available: https://www.iso.org/standard/31432.html. [Accessed 28 03 2017].

[7] "ISO/IEC 7816-4:2013," Internation Organization for Standardization, [Online]. Available: https://www.iso.org/standard/54550.html.

[8] "Common Access Card [CAC]," Department of Defense, [Online]. Available: http://www.cac.mil/common-access-card/.

[9] "E.161 : Arrangement of digits, letters and symbols on telephones and other devices that can be used for gaining access to a telephone network," [Online]. Available: https://www.itu.int/rec/T-REC-E.161-200102-I/en. [Accessed 28 3 2017].

[10] "About Near Field Communication," Ubitap, [Online]. Available: http://www.ubitap.com/whatisnfc.

[11] "NFC A vs NFC B vs NFC F-Difference between NFC-A,NFC-B,NFC-F," RF Wireless World, [Online]. Available: http://www.rfwireless-world.com/Terminology/NFC-A-vs-NFC-B-vs-NFC-F.html.

[12] P. Semiconductors, "13.56 MHz RFID Proximity Antennas," [Online]. Available: http://www.nxp.com/documents/application_note/78010.pdf.

[13] Wikipedia, "Manchester code," [Online]. Available: https://en.wikipedia.org/wiki/Manchester_code.

[14] "Tag Type Specifications," NFC Forum, [Online]. Available: http://nfc-forum.org/our-work/specifications-and-application-

documents/specifications/tag-type-technical-specifications/.

[15] "ISO/IEC 14443-3:2016," International Organization for Standardization, [Online]. Available: https://www.iso.org/standard/70171.html.

[16] "Fingerprint Patterns," Online Digital Education Connection, [Online]. Available: http://www.odec.ca/projects/2004/fren4j0/public_html/fingerprint_patterns.htm.

[17] Biometric Solutions, "Fingerpring Recognition," [Online]. Available: http://www.biometric-solutions.com/fingerprint-recognition.html.

[18] androidauthority.com, "How fingerprint sensors work," [Online]. Available: http://www.androidauthority.com/how-fingerprint-scanners-work-670934/.

[19] National Institute of Standards and Technology, "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & tattoo," in *NIST Special Publication 500-245*, National Institute of Standards and Technology, 2000.

[20] E. Winer, "Real Traps - Measuring Absorption," Real Traps, [Online]. Available: http://realtraps.com/art_measure.htm. [Accessed 30 March 2017].

[21] Acoustiguard Sound and Vibration Guard, "Mass Loaded Vinyl," Acoustiguard, [Online]. Available: http://www.acoustiguard.com/products/soundproofing-walls-ceilings/mass-loaded-vinyl.html. [Accessed 29 March 2017].

[22] Fairchild, "FQP30N06 Data Sheet," [Online]. Available: https://www.fairchildsemi.com/datasheets/FQ/FQP30N06.pdf.

[23] "USB Battery Charging 1.2," [Online]. Available: http://www.usb.org/developers/docs/devclass_docs/USB_Battery_Charging_1.2.pdf.

[24] P. B. A. A.-W. Mark Melodia, "Legal Risks and Rules of hte MOve to Biometrics," *New York Law Journal,* pp. 1-2, 2015.

[25] Law360, "State Forays INto the Regulation of Biometric Data," [Online]. Available: https://www.law360.com/articles/724349/state-forays-into-the-regulation-of-biometric-data.

[26] Illinois General Assembly, "(740 ILCS 14/) Biometric Information Privacy Act.," 3 10 2008. [Online]. Available: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[27] N. F. P. Association, "Chapter 52 Stationary Storage Battery Systems," [Online]. Available: http://codesonline.nfpa.org/a/c.ref/ID00001131314/chapter.

[28] How Stuff Works, "Capacitance Scanners - How Fingerprint Scanners Work," [Online]. Available: http://computer.howstuffworks.com/fingerprint-scanner3.htm.

[29] "ISO/IEC 18000-3:2010," International Organization for Standardization, [Online]. Available: https://www.iso.org/standard/53424.html.

[30] "Fingerprint Recognition," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Fingerprint_recognition#/.

8.2 Data sheets

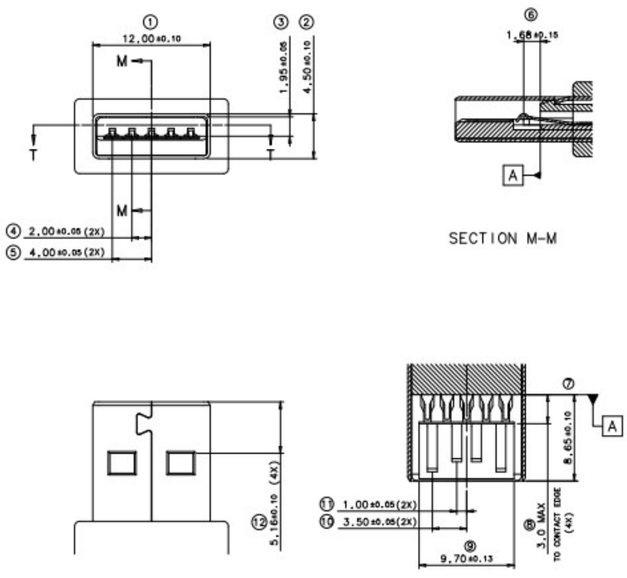
This appendix is for partial data sheets that are referenced within our project.

8.2.1 USB Specification Partial Data Sheet

USB 3 Cable & Connector Compliance Document Revision 1.02

Appendix A Critical Dimensions

A.1 USB 3.0 Standard "A" Plug



USB3.0 STANDARD A CABLE PLUG CONNECTOR CRITICAL DIMENSIONS:

DESCRIPTION	DIMENSION	+ TOL	- TOL
1. PLUG WIDTH	12.00	0.10	-0.10
2. PLUG HEIGHT	4.50	0.10	-0.10
3. PLUG OPENING	1.95	0.05	-0.05
4. SS CONTACT PITCH	2.00	0.05	-0.05
5. SS CONTACT PITCH	4.00	0.05	-0.05
6. SS CONTACT LOCATION	1.68	0.15	-0.15
7. PLUG DEPTH	8.65	0.10	-0.10
8. BLADE LENGTH	3.00	0.00	N/A
9. PLASTIC WIDTH	9.70	0.13	-0.13
10.BLADE PITCH	3.50	0.05	-0.05
11.BLADE PITCH	1.00	0.05	-0.05
12.LATCH OPENING	5.16	0.10	-0.10

All Values are in Millimeters

8.2.2 ATmega328 I/O Pin Output Voltage vs Source Current

Figure 31-307. ATmega328: I/O Pin Output Voltage vs. Source Current (Vcc = 3 V)

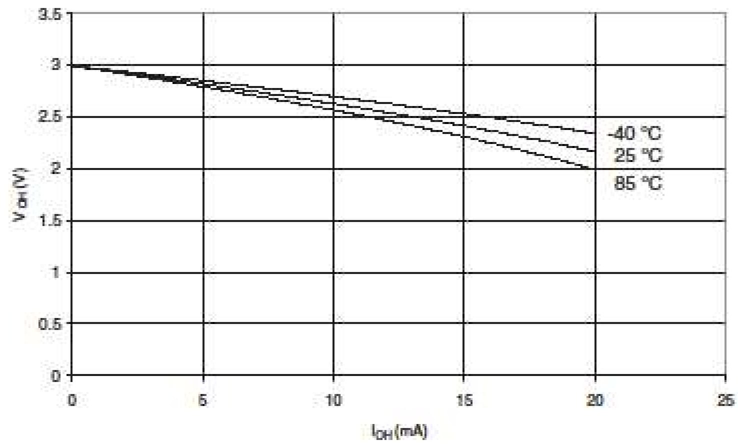
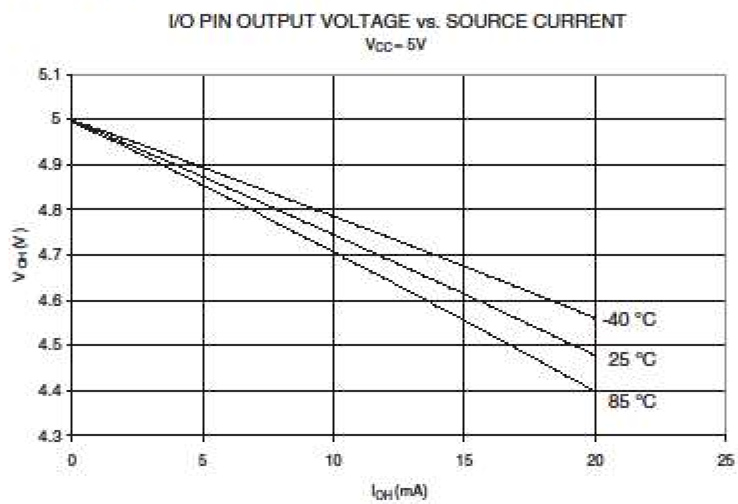


Figure 31-308. ATmega328: I/O Pin Output Voltage vs. Source Current (V_{CC} = 5 V)



ATmega48A/PA/88A/PA/168A/PA/328/P [DATASHEET] 480
Atmel-8271J-AVR- ATmega-Datasheet_11/2015

8.3 **Copyright Permission Requests**

Shown below are copyright permission requisitions. They are in order based on when they appear in our document.

Permission request from How Stuff Works [28]

Reason:

Request Permission to Reprint Articles, Art, Podcasts or Videos

Your Name: Ian Flemings

Your E-mail: Ian.flemings.1989@ieee.org

Message: (400 character limit)

Hello I am a student at the University of Central FLorida and I am currently working on with a group on our Senior Design project to create a remote cell phone charging security notification system. I am requesting permission to use your capacitance scanner image from the document below
URL:http://computer.howstuffworks.com/fingerprint-scanner3.htm

Respectfully,
Ian Flemings

Send the Message

Figure 89 - Copyright request for capacitance fingerprint scanner schematic

Permission request from USB.org

M Me
5:01 PM

Copyright Permission Request
To: admin@usb.org

Hello, I am a student at the University of Central Florida and I am currently working with a group on our Senior Design project to create a remote cell phone charging security notification system. I am requesting permission to use your image:

Figure 4-2 from the Battery Charging Specification Revision 1.2.

Respectfully,
Ian Flemings

Figure 90 - Copyright Permission Request for DCP Required Operating Range Image

8.4 Index